THE YEAR 2000 COMPUTER PROBLEM: LESSONS LEARNED FROM STATE AND LOCAL EXPERIENCES

HEARINGS

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

AUGUST 13, 14, AND 17, 1999

Serial No. 106–48

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE
60–954 CC WASHINGTON : 1999

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. McHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
DAVID M. McINTOSH, Indiana
MARK E. SOUDER, Indiana
JOE SCARBOROUGH, Florida
STEVEN C. LaTOURETTE, Ohio
MARSHALL "MARK" SANFORD, South Carolina
BOB BARR, Georgia
DAN MILLER, Florida
ASA HUTCHINSON, Arkansas
LEE TERRY, Nebraska
JUDY BIGGERT, Illinois
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin
HELEN CHENOWETH, Idaho
DAVID VITTER, Louisiana

HENRY A. WAXMAN, California
TOM LANTOS, California
ROBERT E. WISE, Jr., West Virginia
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
CHAKA FATTAH, Pennsylvania
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
HAROLD E. FORD, Jr., Tennessee
JANICE D. SCHAKOWSKY, Illinois

———

BERNARD SANDERS, Vermont (Independent)

Kevin Binger, *Staff Director*
Daniel R. Moll, *Deputy Staff Director*
David A. Kass, *Deputy Counsel and Parliamentarian*
Carla J. Martin, *Chief Clerk*
Phil Schiliro, *Minority Staff Director*

———

Subcommittee on Government Management, Information, and Technology

STEPHEN HORN, California, *Chairman*

JUDY BIGGERT, Illinois
THOMAS M. DAVIS, Virginia
GREG WALDEN, Oregon
DOUG OSE, California
PAUL RYAN, Wisconsin

JIM TURNER, Texas
PAUL E. KANJORSKI, Pennsylvania
MAJOR R. OWENS, New York
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York

Ex Officio

DAN BURTON, Indiana
HENRY A. WAXMAN, California

J. Russell George, *Staff Director and Chief Counsel*
Bonnie Heald, *Professional Staff Member*
Grant Newman, *Clerk*

CONTENTS

THE YEAR 2000 COMPUTER PROBLEM: LESSONS LEARNED FROM STATE AND LOCAL EXPERIENCES

FRIDAY, AUGUST 13, 1999

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY,
COMMITTEE OF GOVERNMENT REFORM,
Sacramento, CA.

The subcommittee met, pursuant to notice, at 9 a.m., in the Sacramento Board of Supervisors Chambers, room 1450, 700 H Street, Sacramento, CA, Hon. Steve Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn and Ose.

Staff present: J. Russell George, staff director and chief counsel; Bonnie Heald, director of communications and professional staff member; and Grant Newman, clerk.

Mr. HORN. I'm Steve Horn, the chairman of the House Subcommittee on Government Management, Information, and Technology. The presiding officer today will be Mr. Ose, who is a valued member of this committee and represents part of this area as we go north, I guess, from Sacramento a little bit and various other areas. And I'm just going to make an opening statement and then he's going to preside. And I will have the opportunity to ask some questions. He will, too. And we have an excellent panel today which should give a real good feel for where we are in government, at least in California and with some of the private utilities and others.

The hearing is in order as a quorum is present, and I, of course, thank Mr. Ose and the staff for all they've done to make this a very pleasant visit in my home State of California. I represent the area from Long Beach, CA, and I grew up in northern California where I still have a ranch at San Juan Batista. So when I got off the plane a few years ago when I was university president, a lady came up to me and I don't know how she ever knew I ever had anything to do with anything, and she said, "You're stealing our water."

So I understand northern California, the views. It's tough to get water; and believe me, when you have a ranch, it's even tougher.

The year 2000 computer problem, which is the subject of today's hearing, affects nearly every aspect of operations in the government and the private sector and, therefore, impacts all of us.

From Social Security and Medicare to telephone service and electric power, the year 2000 computer bug is the largest management and technology change and challenge that we as a community and as a Nation have confronted. No single organization, city or State, can solve the problem alone, nor can they guarantee their computers will work until the organizations and agencies that exchange data with them are also compliant.

Almost all of the agencies now report their critical computer systems have been renovated. These are the computer systems that must continue functioning in order for Federal agencies to provide their services. That is only part of the complex job that lies ahead. The agency must now complete systemwide testing to ensure that these are renovated and new computers are compatible with other computer systems. As most computer students know, when you tinker with one area of a computer system, you can create unexpected problems in another area.

The problem was created in the mid-1960’s when many of you know, at least my age, you had computers which filled a room of this size, and they had very little memory. The laptop you get now has as much memory as that whole room of computers. And somebody said, “Hey, why are we punching in a four-digit year?” Instead of 1967, let’s just say 67 and knock the 19 off. And, that gained them some memory. I was running the university then, and I’m well aware of the really difficult time we had to get enough memory. And of course, they knew even then that in the year 2000 it would be 00, not 2000, and that would confuse the computer to get either 1900 or 2000, and they wouldn’t know what to do. It would just be simply 00.

So some attention was given to this early on in the 1980’s, and we had one department where a very able programmer told all of the brass, “Hey, we’ve got to start work on this. This is 1987.” They never did a thing. They are still getting If’s, once we got into this in 1996. It’s been very slow.

That’s the Department of Transportation and obviously FAA is the key aspect there. They’re moving ahead. They’ve got an excellent Administrator that’s picked up the pieces that hadn’t been picked up in years. And the other group that had done it on its own was the Social Security Administration. They knew we looked ahead to 1989 that we’ve got to deal with it because we’ve got 50 million different customers here for one program and 43 for another one. And they did it all on their own. There was no precedential guidance in budget and management and they just did it.

And, therefore, they’ve been the first to really be 100 percent compliant, and we shouldn’t have any problems on that front. And 3 years ago we started our first hearing, which was roughly April 1996. And we’ve held about 30 hearings and issued about eight report cards monitoring the status of the executive branch of the Federal Government.

We wrote the President in 1997. We said, “You’ve got to appoint somebody to coordinate this full-time within the executive branch.” He acted on that. That was 1997; he acted on it in 1998. And, in effect, Mr. Koskinen took office in April 1998. He’s done a very fine job. He’s pulled a lot of people together. They are also working with the industrial sector and various panels and so forth. So all of that has been helpful.

At our first hearing we asked the Gardner Group, “How much you think it’s going to cost the Federal Government and nation?” They said, “Well, it’s $600 billion worldwide problem. We’re half the computers in the world, so it will be about $300 billion. That’s the private sector and State and local government.” And I said, “How much for the Federal Government?” They said, “It’s going to cost about $30 billion.”

As I got into this more and more, I thought that was a little high and knew more likely it would be $10 billion. We’re now at the $9 billion mark with the Federal Government through September 30th. We might well use another billion in the last closing panic bit, if there is any of getting the right people in the right place at the right time. It might hit $10 billion. But basically they’ve done it with that amount of $9 billion, and we’re going to have our opening witness with a very fine representative of the General Accounting Office who has kept tabs on the executive branch in their role as the watchdog programmatically and financially on behalf of the legislative branch.

So in addition to programs such as Social Security, Medicare and the Nation’s air traffic control system, 10 of these federally funded programs are operated by the State. These programs which depend on State and county computers, as well as the Federal systems, include Medicaid, food stamps, unemployment insurance, child support enforcement and a myriad of other things. None of the 10 programs will be ready for the year 2000 until December, leaving little if any time to fix unforeseen problems. Data exchanges and interdependencies exist at all levels of government and the private sector. A single failure could disrupt the entire chain of information.

The Social Security Administration, for example, maintains a data base of Social Security payment information for eligible citizens. When these payments are due, the Social Security Administration sends the information to the Department of the Treasury’s Financial Management Service, where the check is issued, and then either electronically deposit it into a personal bank account or deliver it by the U.S. Postal Service.

Each of these agencies has its own network of computers. If even one of them fails, the entire system will break down and the check will not be delivered. Fortunately, the Social Security Administration has been working on this problem for 10 years and it’s in good shape. But even the best prepared computers won’t work without power. Two of the most essential questions involving the year 2000 challenge are, will the lights stay on and the gas pumps remain full. For without electricity and fuel, farm crops cannot move from field to table and commerce cannot flow from factory to household.

The year 2000 computer problem also presents other potential threats to communities, from computed interrupting services, such as 911, to delays in assistance for disasters, such as California’s all too familiar earthquakes, floods, fire, you name it, we do it. Why we are here today is to examine California’s readiness for this challenge as well as the preparations being made by regional local governments and businesses. But even with the best of plans, no one can predict what might or might not happen once the clock ticks midnight this New Year's Eve. The only certainty is that the January 1st deadline cannot be extended.

I understand that California and Sacramento have been working hard toward meeting this deadline. And I welcome today's witnesses and look forward to the testimony.

And with that, Mr. Ose will preside and Chair as the chairman pro tem. He's a valued member of our committee in Washington. Since we're in his district, he's going to chair it and run us through it, and I will ask some questions and so will he.

Does the gentleman from California have an opening statement?

[The prepared statement of Hon. Stephen Horn follows:]

[illegible]
CHAIRMAN

NJAMIN A. GILMAN, NEW YORK
NSTANCE A. MORELLA, MARYLAND
RISTOPHER SHAYS, CONNECTICUT
ANA ROS-LEHTINEN, FLORIDA
HN M. McHUGH, NEW YORK
EPHEN HORN, CALIFORNIA
HN L. MICA, FLORIDA
OMA[illegible] DAVIS III, VIRGINIA
VID [illegible] ITOSH, INDIANA
ARK [illegible] JER, INDIANA
E SCA[illegible]ROUGH, FLORIDA
EVEN C. LATOURETTE, OHIO
ARSHALL "MARK" SANFORD, SOUTH CAROLINA
OB BARR, GEORGIA
AN MILLER, FLORIDA
SA HUTCHINSON, ARKANSAS
E TERRY, NEBRASKA
JDY BIGGERT, ILLINOIS
REG WALDEN, OREGON
OUG OSE, CALIFORNIA
AUL RYAN, WISCONSIN
OHN T. DOOLITTLE, CALIFORNIA
ELEN CHENOWETH, IDAHO

ONE HUNDRED SIXTH CONGRESS

Congreſs of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

MAJORITY (202) 225-5074
MINORITY (202) 225-5051
TTY (202) 225-6852

[illegible]
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
ROBERT E. WISE, JR., WEST VIRGINIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
GARY A. CONDIT, CALIFORNIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
CHAKA FATTAH, PENNSYLVANIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
ROD R. BLAGOJEVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
HAROLD E. FORD, JR., TENNESSEE

BERNARD SANDERS, VERMONT,
INDEPENDENT

"Is California and Sacramento Year 2000 Ready?
Opening Statement of Chairman Stephen Horn (R-CA)
Subcommittee on Government Management, Information, and Technology
August 13, 1999
Sacramento, California

This hearing of the House Subcommittee on Government Management, Information, and Technology, will come to order. I would like to welcome and thank Congressman Doug Ose for being such a gracious host during the subcommittee's visit in Sacramento, the capital of my home state of California.

The Year 2000 computer problem affects nearly every aspect of operations in the government and the private sector and, therefore, impacts every one of us.

From Social Security and Medicare to local telephone service and electric power, the Year 2000 computer bug is the largest management and technological challenges that we as a community and as a nation are likely to confront. No single organization, nor city or state can solve this problem alone. Nor can they guarantee their computers will work, despite the date change, until all organizations and agencies with which they exchange data are also compliant.

The problem was created in the mid-1960s when programmers, seeking to conserve limited computer storage space, began designating the year in two digits rather than four. The year 1967, for example, was shortened to "67." The concern as we approach the new millennium is that computers will misinterpret the last two zeroes in the year 2000 as 1900, causing these systems to malfunction, corrupt data, or shutdown completely.

More than three years ago, our subcommittee held its first congressional hearing on the Year 2000 problem. Since then, we have held nearly 30 hearings and issued 8 "report cards," monitoring the Year 2000 status of the 24 largest agencies in the executive branch of the Federal Government. We selected these agencies because their combined programs directly or indirectly affect the lives of nearly every American.

Almost all of the agencies now report that their critical computer systems have been renovated. These are the computer systems that must continue functioning in order for Federal agencies to provide their services. But that is only part of the complex job that lies ahead. The agencies must now complete systemwide testing to ensure that these renovated or new computers are compatible with other computer systems. As most computer students know, when you tinker with one area of a computer system, you can create unexpected problems in another area.

Current estimates show that the Federal Government will spend nearly $9 billion dollars to fix its computer systems. Several years ago, I predicted the cost would rise to $10 billion dollars. Apparently, I was on target.

Recently, the President's Office of Management and Budget identified 43 Federal programs that provide the most critically needed services to American citizens. In addition to programs such as Social Security, Medicare, and the nation's Air Traffic Control system, 10 of these Federally funded programs are operated by the states. These programs, which depend on state and county computers as well as the Federal systems, include Medicaid, Food Stamps, Unemployment Insurance, and Child Support Enforcement as well as others. None of the 10 programs will be ready for the Year 2000 until December, leaving little, if any, time to fix unforeseen problems.

Data exchanges and interdependencies exist at all levels of government and the private sector. A single failure could disrupt the entire chain of information.

For example, the Social Security Administration maintains a database of Social Security payment information for eligible citizens. When payments are due, the Social Security Administration sends that information to the Department of the Treasury's Financial Management Service where the check is issued and then either electronically deposited into a person's bank account or delivered by the U.S. Postal Service. Each of these agencies has its own network of computers. If even one of them fails, the entire system breaks down and the check will not be delivered.

Fortunately, the Social Security Administration has been working on this problem for 10 years and is in good shape.

But, for computers to continue working, they need power. Two of the most essential questions concerning the Year 2000 challenge are: "Will the lights stay on and the gas pumps remain full?" For without electricity and fuel, farm crops cannot move from field to table and commerce cannot flow from factory to household.

Year 2000 computer problems also present other potentially serious threats to communities, from interruptions in services, such as 911 to delays in assistance for emergencies or disasters such as California's all-too-familiar earthquakes.

We are here today to examine California's readiness to this challenge, and the state of preparedness among regional and local governments and businesses.

Despite the best of plans, no one can predict what may or may not happen once the clock ticks past midnight this New Year's Eve. The only certainty is that this deadline cannot be extended.

I understand that California and Sacramento's government have been working hard to meet this deadline. I welcome today's witnesses and look forward to their testimony.

Mr. OSE. I do, Mr. Chairman.

First of all, let me thank you for coming all this distance to visit with us today. Your work on this subject has been the backbone of everything we're trying to do to make sure this does not become a problem. As arcane as the subject is, the country owes you a great debt of gratitude.

First, I'd like to thank everyone for joining us today at this special field hearing. Today we are going to look at how State and local government entities, utilities and selected businesses in the community have prepared their computer systems for the next century.

On the Federal level, this committee has reviewed the Federal Government's Y2K preparations for several years under the guidance of Chairman Horn. So far this year, it's a long title, but the Government Reform Committee's Government Management, Information, and Technology Subcommittee, of which Mr. Horn is chairman and on which I sit, has held over a dozen hearings on the Y2K computer problem.

As Chairman Horn contends, the Federal Government has been slow to act on the problem. As a result, some of the agencies have had to work overtime to become compliant with the challenge. At this point, about 94 percent of the government's mission-critical systems will be ready for January 1st—excuse me, are ready for January 1st. And the remaining 6 percent have yet to be completed.

The purpose of this hearing, again, is to look beyond the Federal Government and see how localities are dealing with this problem. On the State level, it appears that the State of California's followed a similar path as the Federal Government identifying the problem and going to work on it.

The State Auditor prepared a report in February 1999 and the director of the Department of Information Technology is here with us today to discuss it. As in the Federal Government, the State is hustling, if you will, to make sure that their systems comply as of the end of the year, and I'm looking forward to this testimony.

I'm also pleased to see that we have a wide variety of witnesses who will testify before us today. We'll hear from the representative of Sacramento County and from the Sacramento County Emergency Services. We have someone from my city, the city of Citrus Heights. We'll have a representative from the Regional Council of Rural Counties, and finally from the Government Accountability Office.

We're also going to receive testimony from utility providers, those being PG&E, Pacific Bell, and SMUD. Finally, we'll hear from important industries on the private side such as banking, agriculture, and health care.

I look forward to everyone's testimony, and I hope this hearing will help educate the public on our region's preparedness for the year 2000.

[The prepared statement of Hon. Doug Ose follows:]

DOUG OSE
THIRD DISTRICT, CALIFORNIA

AGRICULTURE COMMITTEE

BANKING AND FINANCIAL
SERVICES COMMITTEE

GOVERNMENT REFORM
COMMITTEE

Congreſs of the United States
Houſe of Repreſentatives
Waſhington, DC 20515–0503

WASHINGTON OFFICE
1508 LONGWORTH HOUSE OFFICE BUILDING
WASHINGTON DC 20515
(202) 225-5716
FAX (202) 226-1298

DISTRICT OFFICE
722-B MAIN STREET
WOODLAND, CA 95695
(530) 669-3540
(916) 489-3684
FAX (530) 669-1395

www.house.gov/ose
doug.ose@mail.house.gov

Congressional Y2K Field Hearing
Subcommittee on Government Management, Information, and Technology

Opening Statement for Congressman Doug Ose

I'd like to thank everyone for joining us for this special Y2K field hearing. Today we are going to look at how state and local government entities, utilities and selected businesses have prepared their computer systems for the next century.

On the Federal level, this Committee has reviewed the Federal Government's Y2K preparations for several years. So far this year, the Government Reform Management, Information, and Technology Subcommittee has held over a dozen hearings on the Y2K computer problem. As Chairman Horn can attest, the Federal Government was slow to act on the problem. As a result, agencies had to work overtime to become Y2K compliant. At this point, about 94% of the government's mission critical systems are ready for January 1st.

The purpose of this hearing is to look beyond the Federal Government and see how localities are dealing with the problem. On the state level, it appears the State of California has followed a similar path as the Federal Government. The California State Auditor reported in February 1999 that the state was woefully behind in many aspects of Y2K preparedness. As a result, the state has had to play catch-up.

I am pleased to see that we have a wide variety of witnesses who will testify before us today. We will hear from the California Department of Information of Technology, a representative from Sacramento County and from the Sac. County Emergency Services, the City of Citrus Heights, a representative from the Regional Council of Rural Counties, and finally the Government Accountability Office. We will also receive testimony from the utility companies that we all rely on, including PG&E, PacBell, and SMUD. Finally, we will hear from important industries including banking, food supply, and health care.

I look forward to everyone's testimony, and I hope this hearing will help educate the public on our region's preparedness for the Year 2000.

Mr. OSE. I would like to invite the first panel down for their testimony. We're going to have you sit right here with—so those folks, Joel Willemssen, Elias Cortez, Doug Cordiner, Joan Smith, Cathy Capriola if you would come join us down here.

OK. We're going to have Mr. Cortez testify first. He's got a 10 a.m. flight. But before we get into that, this being a congressional oversight hearing, I need to swear the witnesses. Folks, if you'll raise your right hands.

Do you solemnly swear the testimony you will give before this subcommittee will be the truth, the whole truth and nothing but the truth?

Let the record show the witnesses responded in the affirmative.

[Witnesses sworn.]

Mr. OSE. So, Mr. Cortez, you're up. Thank you for joining us.

STATEMENTS OF ELIAS CORTEZ, DIRECTOR, DEPARTMENT OF INFORMATION TECHNOLOGY, STATE OF CALIFORNIA; JOEL WILLEMSSEN, DIRECTOR, CIVIL AGENCIES INFORMATION SYSTEMS, U.S. GENERAL ACCOUNTING OFFICE; DOUG CORDINER, PRINCIPAL AUDITOR, BUREAU OF STATE AUDITS, CALIFORNIA STATE AUDITOR'S OFFICE; JOAN SMITH, SUPERVISOR, SISKIYOU COUNTY, ON BEHALF OF THE REGIONAL COUNCIL OF RURAL COUNTIES; AND CATHY CAPRIOLA, ADMINISTRATIVE SERVICES DIRECTOR, CITY OF CITRUS HEIGHTS

Mr. CORTEZ. Good morning. Honorable chair and members, on behalf of Governor Davis, I welcome you and your committee to the State of California.

I am Elias Cortez, chief information officer for the State of California and director of the Department of Information Technology. I would like to thank the members of the subcommittee and all your staff for the opportunity to deliver a brief statement on California's comprehensive year 2000 program. Based on recent reviews and detailed analysis of the Y2K program, efforts not only within the State, but across the Nation, we're confident that California's approach to the year 2000 issue is progressive and comprehensive.

The executive order D–3–99, signed by Governor Gray Davis in February 1999, identified the Y2K issues as the State's No. 1 information technology priority. This emphasizes and ensures that the State's resources are focused on public safety, economic stability, continuation of business, and the uninterrupted delivery of essential government services to all of California's citizens and business partners. The executive order empowered me to lead and make bold, decisive initiatives to assess, validate, and communicate the status of Y2K remediation and preparedness activities.

The executive order also empowered me with authority over all information technology units and resources within the State. Through this role, I forged successful partnerships with representatives of both the public and private sectors, including local governments and State governments and other State entities such as the Governor's Office of Emergency Services, and various committees and task forces convened by the Governor.

Our main purpose and focus was to accelerate and escalate a progressive and successful year 2000 program, and included are sub-committees such as the year 2000 executive committee, year 2000 business economy task force, the year 2000 business council, the year 2000 emergency preparedness task force, and the year 2000 communications and outreach task force. As we implemented and enhanced our year 2000 program in February 1999, we found that government entities were not as prepared as we had thought or had been previously reported, and as a result, we immediately accelerated and escalated our year 2000 program through the proactive implementation of a statewide program management office for Y2K and the development of prescriptive methodologies based on the industry best practices for Y2K.

This approach is documented in the Department of Information Technology's Strategic Plan, which is included in the documents supplied to you. California's year 2000 program is a comprehensive approach to the year 2000 remediation and preparedness and includes the establishment of baseline status for more than a 100-plus State entities, an assessment of each entity, a high-level analysis and the assessment results, and the independent validation and verification of those entities with a mission-critical system's focus by external vendors.

The assessment and review outcomes are tracked through a corrective action planning process. This process ensures accountability and action and focus from the entities with the corrective action plans and resources in place that they are required to complete prior to September 1, 1999. A compilation of the State Department Status Information is presented for review on-line on the web on the California Y2K website, which is www.year2000.ca.gov. This bold-step initiative allows any government entity or citizen to access objective, quantitative, current information about State entities' Y2K efforts.

Additionally, the website information communicates entity status to business partners within and external to the State government entity and structure. California's Y2K program has a significant commitment to ensuring that business continuity and contingency planning occurs for all entities.

The year 2000 management program office, the statewide program, must receive a completed and tested plan from each entity prior to October 1999. The commitment to business continuity and contingency planning echoes a message of Governor Davis' executive order and ensures a seamless delivery of services in order to make the century change a nonevent.

In addition to technical assessments and reviews, our Y2K program consists of extensive communication and outreach activities. These include year 2000 emergency preparedness and business continuity and contingency planning, conferences, infrastructure industry roundtables, legislative-sponsored attendance in hearings in which we participated; additional activities are anticipated over the coming months and the new year relative to communications and outreach on Y2K.

Finally, we have raised the bar regarding end to end testing. We will broaden and strengthen interface testing of data with all our partners in local government to ensure that mission-critical public safety, health and welfare and education services are delivered uninterrupted into the new year.

We have a successful and productive collaboration with counties and local governments and even private sector organizations relative to the services that we deliver from the State. All Y2K activities conducted by the State of California are a direct reflection to the decisive actions taken in support of Governor Davis' administration and the legislature, as well as an unprecedented cooperation among State government entities and partners for the State.

Recent accomplishments by the program will allow the State to ensure continuity of State and county mission critical services to the community at large regardless of unforeseen information system impacts.

I'm extremely confident that California can and will deliver the mission-critical services for residents before, during and after the century event.

In summary, the State has been extremely proactive and focused on California's expectations of uninterrupted services by doing the following things:

We focused in the area of addressing the most challenging issues and mission-critical priorities first and concentrating on the greatest impacts to health, safety and revenues. We've maintained public trust in the infrastructure that Californians depend on by accurately reporting the progress made and any challenges facing forward, managing those to date, making sure that there is a workable solution in place to provide uninterrupted service if an unforeseen year 2000 event occurs, preparing for the unexpected year 2000 related impacts by anticipating scenarios and directing the resources necessary to maintain confidence in our communities via the Office of Emergency Services.

Again, thank you for giving the State the opportunity to testify before you about our comprehensive year 2000 program. We are proud not only to share our current status, but we have proactively shared our methodologies with all local government, small business and entities relative to Y2K.

Thank you.

[The prepared statement of Mr. Cortez follows:]

State of California's Year 2000 Program
July 22, 1999

Executive Summary

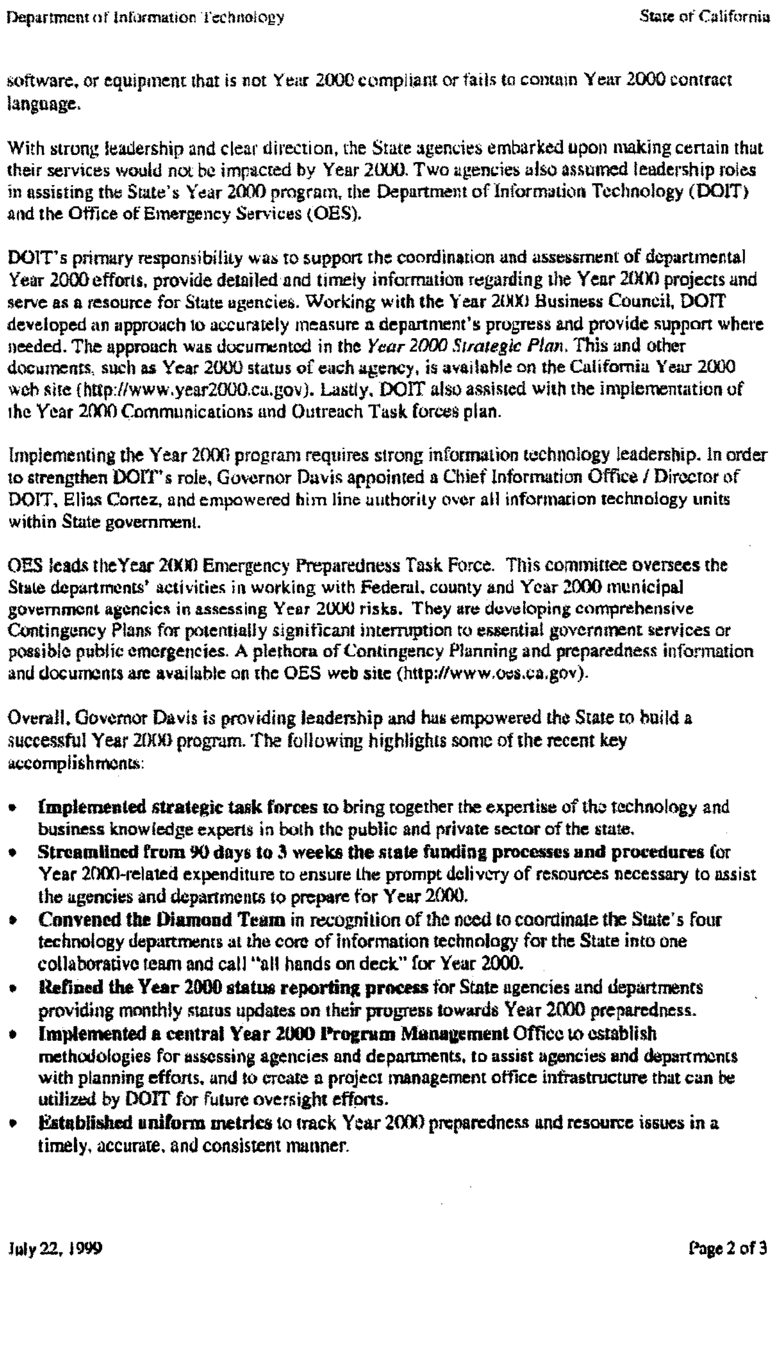
One of the first actions taken by Governor Davis, upon taking office in January 1999, was to make the Year 2000 challenge the top technology priority for the State. With 12 months left until the deadline, aggressive steps were taken to immediately address the daunting task. The commitment and resolve that has been put forth is unsurpassed by any other technology endeavor in the history of the State of California.

Governor-elect Davis initially established a "Transition Team" for information technology in December 1998. The transition team consisted of six strategic and senior technology executives from the public and private sector. This team's objective was to conduct an assessment, develop initial strategies and make recommendations on the new Administration's transition into the effective use of technology in State of California. Given the immediacy of the Year 2000 challenge, however, the team focused on the Department of Information Technology (DOIT) and the State's remediation progress.

In February of 1999, Governor Davis signed Executive Order D-3-99, establishing Year 2000 committees, task forces, councils, and assigning responsibilities and authority to State agencies. The following summarizes these entities:

- *Year 2000 Executive Committee* to assume statewide leadership, coordination and oversight responsibilities of Year 2000 activities.
- *Year 2000 Business Continuity Task Force* that will create a statewide business continuity plan to address the delivery of essential services relying on the coordination of multiple jurisdictions, and to address potential failures of utilities, water, transportation, telecommunication and emergency services.
- *Year 2000 Business Council* to provide ongoing review of the State's Year 2000 strategies, plans and progress and to contribute best practices and proven solutions.
- *Year 2000 Program Management Office* to coordinate and assess departmental Year 2000 efforts, provide detailed and timely information regarding the Year 2000 projects and serve as a resource for State agencies. The Year 2000 Program Management Office works at the direction of the Year 2000 Executive Committee and is supported by the Department of Information Technology.
- *Year 2000 Emergency Preparedness Task Force* to guide State agencies and to work with federal, county and municipal governments in assessing Year 2000 risks and developing worst-case scenarios that might cause significant interruption to government services or constitute public emergencies. This task force is chaired by the Governor's Office of Emergency Services and is comprised of representatives from public and private sector organizations critical to emergency preparedness.
- *Year 2000 Communications and Outreach Task Force* to coordinate communications to the Public, Legislature and Media.

In addition, the Executive Order escalated the Year 2000 challenge to the State's number one information technology project and halted the purchase of new computers systems, hardware,



software, or equipment that is not Year 2000 compliant or fails to contain Year 2000 contract language.

With strong leadership and clear direction, the State agencies embarked upon making certain that their services would not be impacted by Year 2000. Two agencies also assumed leadership roles in assisting the State's Year 2000 program, the Department of Information Technology (DOIT) and the Office of Emergency Services (OES).

DOIT's primary responsibility was to support the coordination and assessment of departmental Year 2000 efforts, provide detailed and timely information regarding the Year 2000 projects and serve as a resource for State agencies. Working with the Year 2000 Business Council, DOIT developed an approach to accurately measure a department's progress and provide support where needed. The approach was documented in the *Year 2000 Strategic Plan*. This and other documents, such as Year 2000 status of each agency, is available on the California Year 2000 web site (http://www.year2000.ca.gov). Lastly, DOIT also assisted with the implementation of the Year 2000 Communications and Outreach Task forces plan.

Implementing the Year 2000 program requires strong information technology leadership. In order to strengthen DOIT's role, Governor Davis appointed a Chief Information Office / Director of DOIT, Elias Cortez, and empowered him line authority over all information technology units within State government.

OES leads theYear 2000 Emergency Preparedness Task Force. This committee oversees the State departments' activities in working with Federal, county and Year 2000 municipal government agencies in assessing Year 2000 risks. They are developing comprehensive Contingency Plans for potentially significant interruption to essential government services or possible public emergencies. A plethora of Contingency Planning and preparedness information and documents are available on the OES web site (http://www.oes.ca.gov).

Overall, Governor Davis is providing leadership and has empowered the State to build a successful Year 2000 program. The following highlights some of the recent key accomplishments:

- **Implemented strategic task forces** to bring together the expertise of the technology and business knowledge experts in both the public and private sector of the state.
- **Streamlined from 90 days to 3 weeks the state funding processes and procedures** for Year 2000-related expenditure to ensure the prompt delivery of resources necessary to assist the agencies and departments to prepare for Year 2000.
- **Convened the Diamond Team** in recognition of the need to coordinate the State's four technology departments at the core of information technology for the State into one collaborative team and call "all hands on deck" for Year 2000.
- **Refined the Year 2000 status reporting process** for State agencies and departments providing monthly status updates on their progress towards Year 2000 preparedness.
- **Implemented a central Year 2000 Program Management** Office to establish methodologies for assessing agencies and departments, to assist agencies and departments with planning efforts, and to create a project management office infrastructure that can be utilized by DOIT for future oversight efforts.
- **Established uniform metrics** to track Year 2000 preparedness and resource issues in a timely, accurate, and consistent manner.

- **Performed Detailed Departmental Assessments (DDA's)** to baseline departmental progress.
- **Implemented Statewide Year 2000 Independent Verification and Validation** (IV&V) process to ensure that oversight of state efforts is monitored consistently
- **Developed Corrective Action Plans** process to track and monitor corrective action plans resulting from the DDA's which monitor agency/department progress and facilitates resource deployment where required ensuring that all technology components are compliant.
- **Facilitated access to Year 2000 specialty vendors and resources** for use by State agencies and departments to effectively address their remediation and testing needs
- **Established Contingency Planning for Business Plan (CPB) Model and Methodologies** to standardize the level of preparation and reporting associated with continuity and business resumption efforts.
- **Created the Year 2000 HelpDesk** to manage inquiries from state agencies regarding the DDA process that serves as a central coordination point of information to and from Year 2000 PMO stakeholders.
- **Increased Year 2000 awareness in public and private sector** utilizing comprehensive Outreach Programs to educate stakeholders and communicate a message of concern for Year 2000 preparedness and not panic. This includes Year 2000 conferences and hearings that were conducted throughout the State as well as the publishing of a State of California Year 2000 web site.
- **Conducted Year 2000 Partnership Pilot Program** with Merced County to determine the effectiveness of the State's DDA's methodology and toolkit in a local government environment.
- **Established of an Event Center Management (EMC)** to act as a focal point to monitor status of all Year 2000 tasks, provide a state-of-the-art technology testing facility, and act as an emergency response and coordination center during the millennium change.
- **Launching of a Year 2000 Communications and Outreach campaign** that includes public and legislative hearings, conferences, media events, and publications (including the publication of the Year 2000 status of all agencies). The mission is to coordinate accurate and timely information about public safety, economic stability, and the continuation of business service delivery as it relates to the Year 2000 transition.
- **Training the business community in Year 2000 readiness** comprising of training 24 cities between 7/14/98 and 6/8/99, small business jumpstart kits for year 2000 preparedness, and a 38-page booklet entitled Small Business Countdown to Year 2000.
- **Formed a State/County External Interface committee** in a collaborative effort to ensure the continuity of state and county services to the community. The committee has divided into working groups which focus on the areas of interface inventory, testing methodology, acceptance documentation and communications.

These achievements pave the way for a successful Year 2000 Program and establish best practices and lessons learned for beyond year 2000. In order to provide better communication to the public, legislature, and media, the State has published the Year 2000 status of every department in the July 1999 Quarterly Report and also maintains a current and extensive web site for Year 2000 information.

Mr. OSE. Director, if I may, in deference to your time, we're going to ask what few questions we have of you first so that you can catch your plane.

First of all, you mentioned the website that you had, the www.year2000.California.gov. I want to make sure that we've got that correctly identified as www.year2000.ca.gov., right?

Mr. CORTEZ. Yes, sir.

Mr. OSE. So if anybody is watching, that's a first—that's one resource everybody can use.

The other question I have most directly is under Chairman Horn's leadership, one of the things that has been most apparent is that our initial attempts to cure this problem have been changed or governed by agencies' self-examination after the fact. And what I'd like to find out is: There are three particular situations I'm concerned about.

First, is it the agencies themselves who are reporting on their compliance, or do you have an independent third party doing that?

Second, since, say, January 1st, have you seen any material change in the degree of readiness amongst the agencies?

And, finally, as it affects regional and local governments in particular, has the State been able to provide any financial assistance to those levels of government to help them get into compliance?

Mr. CORTEZ. Thank you.

Regarding the agencies, we are very proud to say that that was a concern for our legislature coming in. Again, the program wasn't where we had expected it to be. We did see prior to our acceleration and escalation of this program a need for independent validation of verification. We immediately implemented that program. No entities do self-assessment or self-reporting. We've put that behind us. Our new program not only allows us to do current triages, but we have ongoing statewide program management in which we continually track on a weekly basis and post on line on our web the status of any corrective action plans required for these departments.

Furthermore, we're proud to say we're putting that on the web so that any local government and citizens who have any concerns regarding our compliancy or status can go on line and see positive steps taken, actions that need to be taken, and corrective actions and plans in place and resources with dates proactively displayed. So we are totally having an objective review. It's all external and it's independent. And, again, we have a multitude of vendors that are helping us with that process.

Second, the issue on the degree of readiness, we have seen an extreme acceleration and escalation of the Y2K program, and we've even documented that on line. So when you see the department status, you can see the initial baseline and its actual validation where it was when we started the program and where it currently is. And you can see some major improvement and action items taken care of. So we view this program as extremely successful and have recommended to other local government entities not only the methodology that we use; we post it on line and they can download it and use it as a tool kit for themselves if they don't have resources to hire expensive consultants. And many government entities have taken the opportunity to do so.

And, furthermore, we continually assess on a week-to-week basis and allow the departments to give current status. So, as an example, if a department finds an issue that hadn't been dealt with prior to this, it gets red-flagged again and brought into the loop of the program. So we have a comprehensive review of all issues left to be compliant and complete into the new year.

Regional governments, we have proactively been out in the community working with regional governments sharing our methodologies at no cost to them. We're doing conferences. We are aggressively pursuing a communication and outreach program making sure that our message and their message is in sync with the community. We have proactively worked with the legislature to provide dollars so that we can fund such programs. And, again, at this point, the funding that has been put in place I know has gone to core programs and other programs. Again, at this point, I'm not aware of legislation with additional funding.

Mr. OSE. Chairman Horn.

Mr. HORN. Just one brief question. I know the Governor doesn't run the State education systems here, but increasingly Governors do, and I wondered if you as the chief technology boss of the State have a feel for what's happening on K–12, what's happening at the community college level, what's happening at the California State University level. And we do have one witness from the UC–Davis campus, the medical school, but I wondered what you know about what's happening at the University of California, also.

Mr. CORTEZ. Yes. We are proud to say that we've had the opportunity to work side by side with Assembly Member John Dutra, Chair of the Assembly Information Technology Committee, and we've gone across the State and had hearings like this in similar forums, and we have seen that smaller government entities, not just school districts, have had financial challenges that they recently have come out of, and so their starts with the Y2K program have been late.

I personally have met the leader of the Board of Education for our State and have shared our methodology. We have proactively worked with them on the assessment for their department. They take—all government entities take this challenge seriously, and we are continuously working with them. And as an example, through communications and outreach programs trying to disseminate Y2K status and methodologies through their broadcast system. We do and we have found in again smaller government entities that financial strains have been an issue for them. As we did in one case, a city up in northern California, they used $100,000 reserve plus borrowed $50,000 to complete their Y2K program.

So all in all we've seen a major impetus to get the job done. We've seen many challenges on a different level, and we believe the smaller government entities do need help not only in methodologies, but resources. And they need to shift their own internal resources to get this job done, as we've seen with other local government entities.

Mr. HORN. Well, I appreciate that answer. The State auditor has a representative here after you, and we'll ask him some of the questions, but the statewide audit in February I'm sure was helpful in assessing where you were. I don't know the degree to which

California departments have, say, an inspector general because there's another—at least at the Federal level, another independent authority that can call them as they see them. Are you concerned about the verification of what some of the departments are submitting?

Mr. CORTEZ. Actually, I'm confident to say that we've taken the auditor's report to heart. We welcome all their comments. We aggressively pursued as we have expanded and escalated our program all their issues into our program. We reported to them currently and recently about the program and the status of the program. We do not use self-assessment. We do not believe that's the appropriate measure of Y2K. We have proactively worked with what we call the Y2K Business Council.

Right across the mountains here, we have the leaders in the world on technology. And we are lucky to have used them, and they have committed their CIOs to be our compass and guide for our Y2K program; and we've been able to take industry best practices, procedures, and policies, such as software freezes and other things that are related to a good compliant information project—Y2K information project in place. And so we're confident that not only the recommendations from the Bureau of State Audits we've taken into account and implemented; but, furthermore, we've got an additional set of eyes on our program and advisory to our program and that has embellished our program tremendously.

Mr. HORN. Thank you very much.

Mr. OSE. Director, thank you. Appreciate you coming.

Now to the rest of the panel, I appreciate your patience. That's very courteous to extend that to the director. So we'll just go down the list.

Mr. WILLEMSSEN. Thank you, Congressman, for inviting us here today. Chairman Horn, as requested, I'll briefly summarize our statement on the Y2K readiness for Federal Government, State and local government, in key economic sectors.

Regarding the Federal Government, reports indicate continued progress in fixing, testing and implementing mission-critical systems. Nevertheless, numerous critical systems must still be made compliant and must undergo independent verification and validation. The most recent agency quarterly Y2K reports due to OMB today should provide further information on agency progress. Our own reviews of selected agencies have shown uneven progress and remaining risks in addressing Y2K and, therefore, point to the importance of business continuity and contingency planning.

Even for those agencies that have clearly been Federal leaders such as the Social Security Administration, work still remains to ensure full readiness. If we look beyond individual agencies and systems, the Federal Government's future actions will need to be increasingly focused on making sure that its high priority programs are compliant. In line with this, OMB has identified 43 high-impact programs such as Medicare and food safety. As you know, Mr. Chairman, we're currently reviewing for you the executive branch's progress in addressing these high-impact programs. Available information on the year 2000 readiness of State and local governments indicates, also, that much work remains. For example, according to recently reported information on States, about eight

States had completed implementing less than 75 percent of their mission-critical systems. Further, while all States responding said they were engaged in contingency planning, 14 reported their deadlines for this as October or later.

State audit organizations, including the California State Auditor, as earlier mentioned, have also identified significant Y2K concerns in areas such as testing, imbedded systems, and contingency planning.

Mr. OSE. Mr. Willemssen, just a moment. If everyone would turn off their pagers and cell phones, that would be a great benefit to the witnesses. Thank you.

Mr. WILLEMSSEN. Another area of risk is represented by Federal human services programs administered by States, programs such as Medicaid, food stamps and child support enforcement. Of the 43 high-impact priorities identified by OMB, 10 are State-administered Federal programs such as these. OMB reported data on the systems supporting those kinds of programs show that numerous States are not planning to be ready until close to the end of the year. Further, this is based on data that has not been independently verified.

Recent reports have also highlighted Y2K issues at the local government level. For example, last month we reported on the Y2K status of the 21 largest U.S. cities. On average, these cities reported to us completing work for 45 percent of their key services.

Y2K is also a challenge for the public infrastructure in key economic sectors. Among the areas most at risk are health care and education. For health care we've testified on several occasions on the risks facing Medicare, Medicaid and biomedical equipment. In addition, last month we reported that while many surveys have been completed on the Y2K readiness of health care providers, none of the 11 surveys we reviewed provided sufficient information with which to assess the true status of these providers. For education, last week's report of the President's Council on Y2K conversion indicates that this continues to be an area of concern. For example, according to the council report, many school districts could have dysfunctional information systems because less than one-third of institutions were reporting that their systems were compliant.

That concludes a summary of my statement, and I'd be pleased to address any questions you may have.

[The prepared statement of Mr. Willemssen follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
9:00 a.m. PDT
Friday,
August 13, 1999

YEAR 2000 COMPUTING CHALLENGE

Important Progress Made, Yet Much Work Remains to Ensure Delivery of Critical Services

Statement of Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting us to participate in today's hearing on the Year 2000 problem. According to the report of the President's Commission on Critical Infrastructure Protection, the United States--with close to half of all computer capacity and 60 percent of Internet assets--is the world's most advanced and most dependent user of information technology.[1] Should these systems--which perform functions and services critical to our nation--suffer problems, it could create widespread disruption. Accordingly, the upcoming change of century is a sweeping and urgent challenge for public- and private-sector organizations alike.

Because of its urgent nature and the potentially devastating impact it could have on critical government operations, in February 1997 we designated the Year 2000 problem a high-risk area for the federal government.[2] Since that time, we have issued over 130 reports and testimony statements detailing specific findings and numerous recommendations related to the Year 2000 readiness of a wide range of federal agencies.[3] We have also issued guidance to help organizations successfully address the issue.[4]

Today I will highlight the Year 2000 risks facing the nation; discuss the federal government's progress and challenges that remain in correcting its systems; identify state and local government Year 2000 issues; and provide an overview of available information on the readiness of key public infrastructure and economic sectors.

[1] Critical Foundations: Protecting America's Infrastructures (President's Commission on Critical Infrastructure Protection, October 1997).

[2] High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

[3] A list of these publications is included as an attachment to this statement. These publications can be obtained through GAO's World Wide Web page at *www.gao.gov/y2kr.htm.*

[4] Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, issued as an exposure draft in February 1997 and in final form in September 1997), which addresses the key tasks needed to complete each phase of a Year 2000 program (awareness, assessment, renovation, validation, and implementation); Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, issued as an exposure draft in March 1998 and in final form in August 1998), which describes the tasks needed to ensure the continuity of agency operations; and Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, issued as an exposure draft in June 1998 and in final form in November 1998), which discusses the need to plan and conduct Year 2000 tests in a structured and disciplined fashion.

THE PUBLIC FACES RISK OF YEAR 2000 DISRUPTIONS

The public faces the risk that critical services provided by the government and the private sector could be severely disrupted by the Year 2000 computing problem. Financial transactions could be delayed, flights grounded, power lost, and national defense affected. Moreover, America's infrastructures are a complex array of public and private enterprises with many interdependencies at all levels. These many interdependencies among governments and within key economic sectors could cause a single failure to have adverse repercussions in other sectors. Key sectors that could be seriously affected if their systems are not Year 2000 compliant include information and telecommunications; banking and finance; health, safety, and emergency services; transportation; power and water; and manufacturing and small business.

The following are examples of some of the major disruptions the public and private sectors could experience if the Year 2000 problem is not corrected.

- With respect to aviation, there could be grounded or delayed flights, degraded safety, customer inconvenience, and increased airline costs.[5]

- Aircraft and other military equipment could be grounded because the computer systems used to schedule maintenance and track supplies may not work. Further, the Department of Defense could incur shortages of vital items needed to sustain military operations and readiness.[6]

- Medical devices and scientific laboratory equipment may experience problems beginning January 1, 2000, if their software applications or embedded chips use two-digit fields to represent the year.

Recognizing the seriousness of the Year 2000 problem, on February 4, 1998, the President signed an executive order that established the President's Council on Year 2000 Conversion, chaired by an Assistant to the President and consisting of one representative from each of the executive departments and from other federal agencies as may be determined by the Chair. The Chair of the Council was tasked with the following Year 2000 roles: (1) overseeing the activities of agencies; (2) acting as chief spokesperson in national and international forums; (3) providing policy coordination of executive branch activities with state, local, and tribal governments; and (4) promoting appropriate federal roles with respect to private-sector activities.

[5] FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998) and Year 2000 Computing Crisis: FAA Is Making Progress But Important Challenges Remain (GAO/T-AIMD/RCED-99-118, March 15, 1999).

[6] Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998).

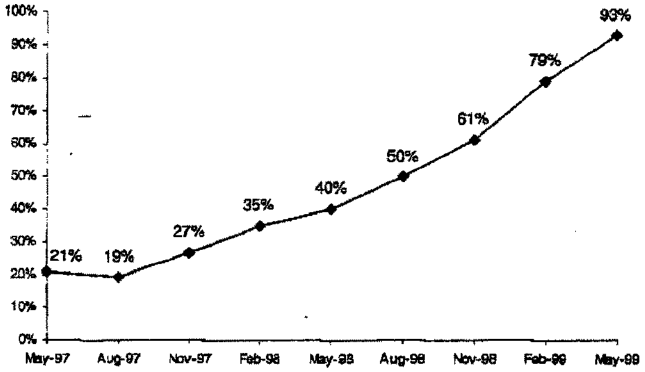
IMPROVEMENTS MADE BUT
MUCH WORK REMAINS

Addressing the Year 2000 problem is a tremendous challenge for the federal government. Many of the federal government's computer systems were originally designed and developed 20 to 25 years ago, are poorly documented, and use a wide variety of computer languages, many of which are obsolete. Some applications include thousands, tens of thousands, or even millions of lines of code, each of which must be examined for date-format problems.

To meet this challenge and monitor individual agency efforts, the Office of Management and Budget (OMB) directed the major departments and agencies to submit quarterly reports on their progress, beginning May 15, 1997. These reports contain information on where agencies stand with respect to the assessment, renovation, validation, and implementation of mission-critical systems, as well as other management information on items such as costs and business continuity and contingency plans.

The federal government's most recent reports show improvement in addressing the Year 2000 problem. While much work remains, the federal government has significantly increased its percentage of mission-critical systems that are reported to be Year 2000 compliant, as chart 1 illustrates. In particular, while the federal government did not meet its goal of having all mission-critical systems compliant by March 1999, as of mid-May 1999, 93 percent of these systems were reported compliant.

Chart 1: Mission-Critical Systems Reported Year 2000 Compliant, May 1997-May 1999



Source: May 1997 – May 1999 data are from the OMB quarterly reports.

While this reported progress is notable, OMB also noted that 10 agencies have mission-critical systems that were not yet compliant.[7] In addition, as we testified in April, some of the systems that were not yet compliant support vital government functions.[8] For example, some of the systems that were not compliant were among the 26 mission-critical systems that the Federal Aviation Administration (FAA) has identified as posing the greatest risk to the National Airspace System—the network of equipment, facilities, and information that supports U.S. aviation operations.

Additionally, not all systems have undergone an independent verification and validation process. For example, in April 1999 the Department of Commerce awarded a contract for independent verification and validation reviews of approximately 40 mission-critical systems that support that Department's most critical business processes. These reviews are to continue through the summer of 1999. In some cases, independent verification and validation of compliant systems have found serious problems. For example, as we testified this past February,[9] none of 54 external mission-critical systems of the Health Care Financing Administration reported by the Department of Health and Human Services (HHS) as compliant as of December 31, 1998, was Year 2000 ready at that time, based on serious qualifications identified by the independent verification and validation contractor.

Reviews Show Uneven Federal Agency Progress

While the overall Year 2000 readiness of the government has improved, our reviews of federal agency Year 2000 programs have found uneven progress. Some agencies had made good progress while other agencies were significantly behind schedule but had taken actions to improve their readiness. For example:

- In October 1997, we reported that while SSA had made significant progress in assessing and renovating mission-critical mainframe software, certain areas of risk in its Year 2000 program remained.[10] Accordingly, we made several recommendations to address these risk areas, which included the Year 2000 compliance of the systems used by the 54 state Disability Determination Services[11] that help administer the disability programs. SSA agreed with these recommendations and, in July 1999, we

[7] The 10 agencies were the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Justice, Transportation, Treasury; the National Aeronautics and Space Administration; and the U.S. Agency for International Development.

[8] Year 2000 Computing Challenge: Federal Government Making Progress But Critical Issues Must Still Be Addressed to Minimize Disruptions (GAO/T-AIMD-99-144, April 14, 1999).

[9] Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services (GAO/T-AIMD-99-92, February 26, 1999).

[10] Social Security Administration: Significant Progress Made in Year 2000 Effort, But Key Risks Remain (GAO/AIMD-98-6, October 22, 1997).

[11] These include the systems in all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.

reported that actions to implement these recommendations had either been taken or were underway.[12] For example, regarding the state Disability Determination Services systems, SSA enhanced its monitoring and oversight by establishing a full-time project team, designating project managers and coordinators, and requesting bi-weekly reports. While actions such as these demonstrated SSA's leadership in addressing the Year 2000 problem, it still needed to complete critical tasks to ensure readiness, including (1) ensuring the compliance of all external data exchanges, (2) completing tasks outlined in its contingency plans, (3) certifying the compliance of one remaining mission-critical system, (4) completing hardware and software upgrades in the Office of Telecommunications and Systems Operations, and (5) correcting date field errors identified through its quality assurance process.

- In May 1999 we testified[13] that the Department of Education had made progress toward addressing the significant risks we had identified in September 1998[14] related to systems testing, exchanging data with internal and external partners, and developing business continuity and contingency plans. Nevertheless, work remained ongoing in these areas. For example, Education had scheduled a series of tests with its data exchange partners, such as schools, through the early part of the fall. Tests such as these are important since Education's student financial aid environment is very large and complex, including over 7,000 schools, 6,500 lenders, and 36 guaranty agencies, as well as other federal agencies; we have reported that Education has experienced serious data integrity problems in the past.[15] Accordingly, our May testimony stated that Education needed to continue end-to-end testing of critical business processes involving Education's internal systems and its external data exchange partners and continue its outreach activities with schools, guaranty agencies, and other participants in the student financial aid community.

- Our work has shown that the Department of Defense and the military services face significant problems.[16] This March we testified that, despite considerable progress made in the preceding 3 months, the department was still well behind schedule.[17] We found that the Department of Defense faced two significant challenges: (1)

[12] Social Security Administration: Update on Year 2000 and Other Key Information Technology Initiatives (GAO/T-AIMD-99-259, July 29, 1999).

[13] Year 2000 Computing Challenge: Education Taking Needed Actions But Work Remains (GAO/T-AIMD-99-180, May 12, 1999).

[14] Year 2000 Computing Crisis: Significant Risks Remain to Department of Education's Student Financial Aid Systems (GAO/T-AIMD-98-302, September 17, 1998).

[15] Student Financial Aid Information: Systems Architecture Needed to Improve Programs' Efficiency (GAO/AIMD-97-122, July 29, 1997).

[16] Defense Computers: Year 2000 Computer Problems Put Navy Operations At Risk (GAO/AIMD-98-150, June 30, 1998); Defense Computers: Army Needs to Greatly Strengthen Its Year 2000 Program (GAO/AIMD-98-53, May 29, 1998); GAO/AIMD-98-72, April 30, 1998; and Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998).

[17] Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed (GAO/T-AIMD-99-101, March 2, 1999).

completing remediation and testing of its mission-critical systems and (2) having a reasonable level of assurance that key processes will continue to work on a day-to-day basis and key operational missions necessary for national defense can be successfully accomplished. We concluded that such assurance could only be provided if Defense took steps to improve its visibility over the status of key business processes.

End-To-End Testing Must Be Completed

While it is important to achieve compliance for individual mission-critical systems, realizing such compliance alone does not ensure that business functions will continue to operate through the change of century—the ultimate goal of Year 2000 efforts. The purpose of end-to-end testing is to verify that a defined set of interrelated systems, which collectively support an organizational core business area or function, will work as intended in an operational environment. In the case of the year 2000, many systems in the end-to-end chain will have been modified or replaced. As a result, the scope and complexity of testing--and its importance--are dramatically increased, as is the difficulty of isolating, identifying, and correcting problems. Consequently, agencies must work early and continually with their data exchange partners to plan and execute effective end-to-end tests. (Our Year 2000 testing guide sets forth a structured approach to testing, including end-to-end testing.)[18]

In January we testified that with the time available for end-to-end testing diminishing, OMB should consider, for the government's most critical functions, setting target dates, and having agencies report against them, for the development of end-to-end test plans, the establishment of test schedules, and the completion of the tests.[19] On March 31, OMB and the Chair of the President's Council on Year 2000 Conversion announced that one of the key priorities that federal agencies will be pursuing during the rest of 1999 will be cooperative end-to-end testing to demonstrate the Year 2000 readiness of federal programs with states and other partners.

Agencies have also acted to address end-to-end testing. For example, our March FAA testimony[20] found that the agency had addressed our prior concerns about the lack of detail in its draft end-to-end test program plan and had developed a detailed end-to-end testing strategy and plans.[21] Also, in June 1999 we reported[22] that the Department of Defense had underway or planned hundreds of related Year 2000 end-to-end test and evaluation activities and that, thus far, it was taking steps to ensure that these related end-to-end tests were effectively coordinated. However, we concluded that the Department of

[18] GAO/AIMD-10.1.21, November 1998.

[19] Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, January 20, 1999).

[20] GAO/T-AIMD/RCED-99-118, March 15, 1999.

[21] GAO/T-AIMD-98-251, August 6, 1998.

[22] Defense Computers: Management Controls Are Critical To Effective Year 2000 Testing (GAO/AIMD-99-172, June 30, 1999).

Defense was far from successfully finishing its various Year 2000 end-to-end test activities and that it must complete efforts to establish end-to-end management controls, such as establishing an independent quality assurance program.

Business Continuity and Contingency Plans Are Needed

Business continuity and contingency plans are essential. Without such plans, when unpredicted failures occur, agencies will not have well-defined responses and may not have enough time to develop and test alternatives. Federal agencies depend on data provided by their business partners as well as on services provided by the public infrastructure (e.g., power, water, transportation, and voice and data telecommunications). One weak link anywhere in the chain of critical dependencies can cause major disruptions to business operations. Given these interdependencies, it is imperative that contingency plans be developed for all critical core business processes and supporting systems, regardless of whether these systems are owned by the agency. Accordingly, in April 1998 we recommended that the Council require agencies to develop contingency plans for all critical core business processes.[23]

OMB has clarified its contingency plan instructions and, along with the Chief Information Officers Council, has adopted our business continuity and contingency planning guide.[24] In particular, on January 26, 1999, OMB called on federal agencies to identify and report on the high-level core business functions that are to be addressed in their business continuity and contingency plans, as well as to provide key milestones for development and testing of such plans in their February 1999 quarterly reports. In addition, on May 13 OMB required agencies to submit high-level versions of these plans by June 15. According to an OMB official, OMB has received plans from the 24 major departments and agencies. This official stated that OMB planned to review the plans, discuss them with the agencies, determine whether there were any common themes, and report on the plans' status in its next quarterly report.

To provide assurance that agencies' business continuity and contingency plans will work if needed, on January 20 we suggested that OMB may want to consider requiring agencies to test their business continuity strategy and set a target date, such as September 30, 1999, for the completion of this validation.[25] Our review of the 24 major departments and agencies' May 1999 quarterly reports found 14 cases in which agencies did not identify test dates for their business continuity and contingency plans or reported test dates subsequent to September 30, 1999.

On March 31, OMB and the Chair of the President's Council announced that completing and testing business continuity and contingency plans as insurance against disruptions to federal service delivery and operations from Year 2000-related failures will be one of the

[23] Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Parternships (GAO/AIMD-98-85, April 30, 1998).
[24] GAO/AIMD-10.1.19, August 1998.
[25] GAO/T-AIMD-99-50, January 20, 1999.

key priorities that federal agencies will be pursuing through the rest of 1999. Accordingly, OMB should implement our suggestion and establish a target date for the validation of agency business continuity and contingency plans.

Our reviews of specific agency business continuity and contingency plans have found that agencies are in varying stages of completion. For example,

- We testified in July 1999 that SSA was in the process of testing all of its contingency plans, with expected completion in September.[26] In addition, SSA planned to assist the Department of the Treasury in developing alternative disbursement processes for problematic financial institutions.

- This June, we testified that the U. S. Customs Service had implemented sound management processes for developing business continuity and contingency plans and was in the process of testing its plans.[27] Customs expected to complete contingency plan testing by October 1999.

- In May 1999, we reported[28] that the Department of Agriculture's component agencies were actively engaged in developing business continuity and contingency plans but that much work remained to complete and test these plans. Further, its December 1999 departmentwide goal of completing business continuity and contingency plans left no room for delays or sufficient time for correcting, revising, and retesting plans, if necessary. Consequently, we recommended that the Department of Agriculture advance its time frame to no later than September 30, 1999, and develop priorities for completing and testing business continuity and contingency plans that are aligned with the department's highest priority business processes, to ensure that remaining work addresses these processes first. The Department of Agriculture's Chief Information Officer stated that the department planned to implement our recommendations.

- This June, we reported[29] that the General Services Administration had completed its telecommunications business continuity and contingency plan in September 1998. However, we made several suggestions for enhancing this plan, including that the General Services Administration work with its customers to ensure that the customers' business continuity and contingency plans are fully coordinated with the General Services Administration's plan and that it consider the possibility of partial loss of service. The General Services Administration agreed to implement our suggestions.

[26] GAO/T-AIMD-99-259, July 29, 1999.

[27] Year 2000 Computing Crisis: Customs Is Making Good Progress (GAO/T-AIMD-99-225, June 29, 1999).

[28] Year 2000 Computing Crisis: USDA Needs to Accelerate Time Frames for Completing Contingency Planning (GAO/AIMD-99-178, May 21, 1999).

[29] GSA's Effort to Develop Year 2000 Business Continuity and Contingency Plans for Telecommunications Systems (GAO/AIMD-99-201R, June 16, 1999).

OMB Action Could Help Ensure Business Continuity of High-Impact Programs

While individual agencies have been identifying and remediating mission-critical systems, the government's future actions need to be focused on its high-priority programs and ensuring the continuity of these programs, including the continuity of federal programs that are administered by states. Accordingly, governmentwide priorities need to be based on such criteria as the potential for adverse health and safety effects, adverse financial effects on American citizens, detrimental effects on national security, and adverse economic consequences. In April 1998 we recommended that the President's Council on Year 2000 Conversion establish governmentwide priorities and ensure that agencies set agencywide priorities.[30]

On March 26, OMB implemented our recommendation by issuing a memorandum to federal agencies designating lead agencies for the government's 42 high-impact programs (e.g., food stamps, Medicare, and federal electric power generation and delivery). (OMB later added a 43rd high-impact program—the Department of Justice's National Crime Information Center.) Appendix I lists these programs and their lead agencies. For each program, the lead agency was charged with identifying to OMB the partners integral to program delivery; taking a leadership role in convening those partners; assuring that each partner has an adequate Year 2000 plan and, if not, helping each partner without one; and developing a plan to ensure that the program will operate effectively. According to OMB, such a plan might include testing data exchanges across partners, developing complementary business continuity and contingency plans, sharing key information on readiness with other partners and the public, and taking other steps necessary to ensure that the program will work. OMB directed the lead agencies to provide a schedule and milestones of key activities in their plans by April 15. OMB also asked agencies to provide monthly progress reports. As you know, we are currently reviewing agencies' progress in ensuring the readiness of their high-impact programs for this subcommittee.

STATE AND LOCAL GOVERNMENTS FACE SIGNIFICANT YEAR 2000 RISKS

Just as the federal government faces significant Year 2000 risks, so too do state and local governments. If the Year 2000 problem is not properly addressed, for example, (1) food stamps and other types of payments may not be made or could be made for incorrect amounts; (2) date-dependent signal timing patterns could be incorrectly implemented at highway intersections, with safety severely compromised; and (3) prisoner release or parole eligibility determinations may be adversely affected. Nevertheless, available information on the Year 2000 readiness of state and local governments indicates that much work remains.

[30] GAO/AIMD-98-85, April 30, 1998.

According to information on state Year 2000 activities reported to the National Association of State Information Resource Executives as of August 3, 1999,[31] states[32] reported having thousands of mission-critical systems.[33] With respect to completing the implementation phase for these systems,

- 2 states[34] reported that they had completed between 25 and 49 percent,
- 6 states[35] reported completing between 50 and 74 percent,
- 38 states[36] reported completing between 75 and 99 percent, and
- 3 states reported completing the implementation phase for all mission-critical systems.[37]

All of the states responding to the National Association of State Information Resource Executives survey reported that they were actively engaged in internal and external contingency planning and that they had established target dates for the completion of these plans; 14 (28 percent) reported the deadline as October 1999 or later.

State audit organizations have also identified significant Year 2000 concerns. In January, the National State Auditors Association reported on the results of its mid-1998 survey of Year 2000 compliance among states.[38] This report stated that, for the 12 state audit organizations that provided Year 2000-related reports, concerns had been raised in areas such as planning, testing, embedded systems, business continuity and contingency planning, and the adequacy of resources to address the problem.

We identified additional products by 17 state-level audit organizations and Guam that

[31] Individual states submit periodic updates to the National Association of State Information Resource Executives. For the August 3 report, over three quarters of the states submitted their data after July 1, 1999. The oldest data were provided on March 11 and the most recent data on August 2.

[32] In the context of the National Association of State Information Resource Executives survey, the term "states" includes the District of Columbia and Puerto Rico.

[33] Mission-critical systems were defined as those that a state had identified as priorities for prompt remediation.

[34] One state reported on its mission-critical systems and one state reported on its processes.

[35] Five states reported on their mission-critical systems and one reported on all systems.

[36] Thirty-one states reported on their mission-critical systems, two states reported on their applications, one reported on its "priority business activities," one reported on its "critical compliance units," one reported on all systems, one reported on functions, and one reported on projects.

[37] Two states did not respond to the survey and one did not respond to this question.

[38] Year 2000: State Compliance Efforts (National State Auditors Association, January 1999).

discussed the Year 2000 problem and that had been issued since October 1, 1998. Several of these state-level audit organizations noted that progress had been made. However, the audit organizations also expressed concerns that were consistent with those reported by the National State Auditors Association. For example:

- In December 1998 the Vermont State Auditor reported[39] that the state Chief Information Officer did not have a comprehensive control list of the state's information technology systems. Accordingly, the audit office stated that, even if all mission-critical state systems were checked, these systems could be endangered by information technology components that had not been checked or by linkages with the state's external electronic partners.

- In April, New York's Division of Management Audit and State Financial Services reported that state agencies did not adequately control the critical process of testing remediated systems.[40] Further, most agencies were in the early stages of addressing potential problems related to data exchanges and embedded systems and none had completed substantive work on contingency planning. The New York audit office subsequently issued 27 reports on individual mission-critical and high-priority systems that included concerns about, for example, contingency planning and testing.

- In March, Oregon's Audits Division reported[41] that 11 of the 12 state agencies reviewed did not have business continuity plans addressing potential Year 2000 problems for their core business functions.

- In March, North Carolina's State Auditor reported[42] that resource restrictions had limited the state's Year 2000 Project Office's ability to verify data reported by state agencies.

With respect to California, in February, the California State Auditor reported[43] that state agencies were making progress in ensuring the uninterrupted delivery of critical services but that many of the 14 agencies that provide the most critical services had not completed

[39] Vermont State Auditor's Report on State Government's Year 2000 Preparedness (Y2K Compliance) for the Period Ending November 1, 1998 (Office of the State Auditor, December 31, 1998).

[40] New York's Preparation for the Year 2000: A Second Look (Office of the State Comptroller, Division of Management Audit and State Financial Services, Report 98-S-21, April 5, 1999).

[41] Department of Administrative Services Year 2000 Statewide Project Office Review (Secretary of State, Audits Division, State of Oregon Report No. 99-05, March 16, 1999).

[42] Department of Commerce, Information Technology Services Year 2000 Project Office (Office of the State Auditor, State of North Carolina, March 18, 1999).

[43] Year 2000 Computer Problem: The State's Agencies Are Progressing Toward Compliance but Key Steps Remain Incomplete (California State Auditor, February 18, 1999).

their Year 2000 efforts. Eleven agencies had not completely tested their computer systems and seven had not corrected or replaced embedded systems. For example, key agencies responsible for emergency services, corrections, and water resources had not fully addressed embedded technology-related threats. Regarding emergency services, the California report stated that if remediation of the embedded technology in its networks were not completed, the Office of Emergency Services might have to rely on cumbersome manual processes, significantly increasing response time to disasters.

It is also essential that local government systems be ready for the change of century since critical functions involving, for example, public safety and traffic management, are performed at the local level. Recent reports on local governments have highlighted Year 2000 concerns. For example:

- On July 15, we reported on the reported Year 2000 status of the 21 largest U.S. cities.[44] On average, cities reported completing work for 45 percent of the key service areas in which they have responsibility. In addition, two cities reported that they had completed their Year 2000 efforts, nine cities expected to complete their Year 2000 preparations by September 30, 1999, and the remaining 10 cities expected to complete their preparation by December 31.[45] In addition, 7 cities reported completing Year 2000 contingency plans, while 14 cities reported that their plans were still being developed.

- On July 9, the National League of Cities reported on its survey of 403 cities conducted in April 1999. This survey found that (1) 92 percent of cities had a citywide Year 2000 plan, (2) 74 percent had completed their assessment of critical systems, and (3) 66 percent had prepared contingency plans. (Of those that had not completed such plans, about half stated that they were planning to develop one.) In addition, 92 percent of the cities reported that they expect that all of their critical systems will be compliant by January 1, 2000; 5 percent expected to have completed between 91 and 99 percent, and 3 percent expected to have completed between 81 and 90 percent of their critical systems by January 1.

- On June 23, the National Association of Counties announced the results of its April survey of 500 randomly selected counties. This survey found that (1) 74 percent of respondents had a countywide plan to address Year 2000 issues, (2) 51 percent had completed system assessments, and (3) 27 percent had completed system testing. In addition, 190 counties had prepared contingency plans and 289 had not. Further, of the 114 counties reporting that they planned to develop Year 2000 contingency plans,

[44] Reported Y2K Status of the 21 Largest U.S. Cities (GAO/AIMD-99-246R, July 15, 1999).

[45] In most cities, the majority of city services are scheduled to be completed before this completion date. For example, Los Angeles plans to have all key city systems ready by September 30, except for its wastewater treatment systems, which are expected to be completed in November.

22 planned to develop the plan in April-June, 64 in July-September, 18 in October-December, and 10 did not yet know.

Of critical importance to the nation are services essential to the safety and well-being of individuals across the country, namely 9-1-1 systems and law enforcement. For the most part, responsibility for ensuring continuity of service for 9-1-1 calls and law enforcement resides with thousands of state and local jurisdictions. On April 29 we testified that not enough was known about the status of either 9-1-1 systems or of state and local law enforcement activities to conclude about either's ability during the transition to the year 2000 to meet the public safety and well-being needs of local communities across the nation.[46] While the federal government planned additional actions to determine the status of these areas, we stated that the President's Council on Year 2000 Conversion should use such information to identify specific risks and develop appropriate strategies and contingency plans to respond to those risks.

We subsequently reported[47] that the Federal Emergency Management Agency and the Department of Justice have worked to increase the response rate to a survey of public safety organizations. As of June 30, 1999, of the over 2,200 9-1-1 sites responding, 37 percent reported that they were ready for the Year 2000. Another 55 percent responded that they expected to be Year 2000 compliant in time for the change of century.

Recognizing the seriousness of the Year 2000 risks facing state and local governments, the President's Council has developed initiatives to address the readiness of state and local governments. For example:

- The Council established working groups on state and local governments and tribal governments.
- Council officials participate in monthly multistate conference calls.
- In July 1998 and March 1999, the Council, in partnership with the National Governors' Association, convened Year 2000 summits with state and U.S. territory Year 2000 coordinators.
- On May 24, the Council announced a nationwide campaign to promote "Y2K Community Conversations" to support and encourage efforts of government officials, business leaders, and interested citizens to share information on their progress. To support this initiative, the Council has developed and is distributing a toolkit that provides examples of which sectors should be represented at these events and issues that should be addressed.

[46] Year 2000 Computing Challenge: Status of Emergency and State and Local Law Enforcement Systems Is Still Unknown (GAO/T-AIMD-99-163, April 29, 1999).
[47] Emergency and State and Local Law Enforcement Systems: Committee Questions Concerning Year 2000 Challenges (GAO/AIMD-99-247R, July 14, 1999).

State-Administered Federal Human Services Programs Are At Risk

Among the critical functions performed by states are the administration of federal human services programs. As we reported in November 1998, many systems that support state-administered federal human services programs were at risk, and much work remained to ensure that services would continue.[48] In February of this year, we testified that while some progress had been achieved, many states' systems were not scheduled to become compliant until the last half of 1999.[49] Accordingly, we concluded that, given these risks, business continuity and contingency planning was even more important in ensuring continuity of program operations and benefits in the event of systems failures.

Subsequent to our November 1998 report, OMB directed federal oversight agencies to include the status of selected state human services systems in their quarterly reports. Specifically, in January 1999, OMB requested that agencies describe actions to help ensure that federally supported, state-run programs will be able to provide services and benefits. OMB further asked that agencies report the date when each state's systems will be Year 2000-compliant.

Table 1 summarizes the latest information on state-administered federal human services programs reported by OMB on June 15, 1999.[50] This information was gathered, but not verified, by the Departments of Agriculture, HHS, and Labor.[51] It indicates that while many states reported their programs to be compliant, a number of states did not plan to complete Year 2000 efforts until the last quarter of 1999. For example, eight states did not expect to be compliant until the last quarter of 1999 for Child Support Enforcement, five states for Unemployment Insurance, and four states for Child Nutrition. Moreover, Year 2000 readiness information was unknown in many cases. For example, according to OMB, the status of 32 states' Low Income Home Energy Assistance programs was unknown because applicable readiness information was not available.

[48] Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998).

[49] Year 2000 Computing Crisis: Readiness of State Automated Systems That Support Federal Human Services Programs (GAO/T-AIMD-99-91, February 24, 1999).

[50] For Medicaid, OMB reports on the two primary systems that states use to administer the program: (1) the Integrated Eligibility System, to determine whether an individual applying for Medicaid meets the eligibility criteria for participation, and (2) the Medicaid Management Information System, to process claims and deliver payments for services rendered. Integrated eligibility systems are also often used to determine eligibility for other public assistance programs, such as Food Stamps.

[51] The Department of Agriculture oversees the Child Nutrition, Food Stamp, and the Women, Infants, and Children programs. HHS oversees the Child Care, Child Support Enforcement, Child Welfare, Low Income Home Energy Assistance, Medicaid, and Temporary Assistance for Needy Families programs. The Department of Labor oversees the Unemployment Insurance program.

Table 1: Reported State-level Readiness for Federally Supported Programs[a]

		Expected Date of 1999 Compliance					
Program[b]	Compliant[c]	Jan.-March	April-June	July-Sept.	Oct.-Dec.	Unk.[d]	N/A[e]
Child Nutrition	29	0	9	10	4	2	0
Food Stamps	25	0	12	14	3	0	0
Women, Infants, and Children	33	0	11	7	3	0	0
Child Care	24	5	5	8	2	6	4
Child Support Enforcement	15	4	13	8	8	6	0
Child Welfare	20	5	9	11	3	5	1
Low Income Home Energy Assistance Program	10	0	3	7	1	32	1
Medicaid – Integrated Eligibility System	20	0	15	15	4	0	0
Medicaid – Management Information System	17	0	19	14	4	0	0
Temporary Assistance for Needy Families	19	3	12	15	1	4	0
Unemployment Insurance	27	0	11	10	5	0	1

[a] This chart contains readiness information from the 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.

[b] According to OMB, the information regarding Child Care, Child Support Enforcement, the Low Income Home Energy Assistance Program, Medicaid, and Temporary Assistance for Needy Families was as of January 31, 1999; and the information for Child Nutrition, Food Stamps, and Women, Infants and Children was as of March 1999. However, OMB provided a draft table to the National Association of State Information Resource Executives which, in turn, provided the draft table to the states. The states were asked to contact HHS and Agriculture and provide corrections by June 1, 1999. For their part, HHS and Agriculture submitted updated state data to OMB in early June. The information regarding Unemployment Insurance was as of March 31, 1999.

[c] In many cases, the report indicated a date instead of whether the state was compliant. We assumed that states reporting completion dates in 1998 or earlier were compliant.

[d] Unknown indicates that, according to OMB, the data reported by the states were unclear or that no information was reported by the agency.

[e] N/A indicates that the states or territories reported that the data requested were not applicable to them.

Source: Progress on Year 2000 Conversion: 9th Quarterly Report (OMB, issued on June 15, 1999).

Although many states have reported their state-administered programs to be compliant, additional work beyond individual system completion likely remains, such as end-to-end testing. For example, of the states that OMB reported as having compliant Medicaid management information and/or integrated eligibility systems, at least four and five states, respectively, had not completed end-to-end testing.

In addition to obtaining state-reported readiness status information for OMB, the three federal departments are taking other actions to assess the ability of state-administered programs to continue into the next century. However, as table 2 shows, the approaches of the three departments in assessing the readiness of state-administered federal human services programs vary significantly. For example, HHS' Health Care Financing Administration (HCFA) hired a contractor to perform comprehensive on-site reviews in all states, some more than once, using a standard methodology. Agriculture's Food and Nutrition Service (FNS) approach includes such actions as having regional offices monitor state Year 2000 efforts and obtaining state certifications of compliance. The Department of Labor is relying on its regional offices to monitor state Year 2000 efforts as well as requiring states to obtain and submit an independent verification and validation report after declaring their systems compliant.

Table 2: Number and Types Of Assessments Performed

		Areas Covered By Assessments		
Agency/Program	Number of States Assessed	Project Management/ Planning	Test Plans/Results	Business Continuity and Contingency Plans (BCCP)
Agriculture/ Child Nutrition Program	Component entity's regional offices are monitoring all states' efforts	Varies by region	Varies by region	Varies by region
Agriculture/ Food Stamps	Component entity's regional offices are monitoring all states' efforts	Varies by region	Varies by region	Varies by region
Agriculture/ Women, Infants, and Children	Component entity's regional offices are monitoring all states' efforts	Varies by region	Varies by region	Varies by region
HHS/Child Care	As of July 2, a contractor had conducted on-site reviews of 20 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—on-site visits included reviews of states' BCCP processes, but not their content
HHS/Child Support Enforcement	As of July 2, a contractor had conducted on-site reviews of 20 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—on-site visits included reviews of states' BCCP processes, but not their content
HHS/Child Welfare	As of July 2, a contractor had conducted on-site reviews of 20 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—on-site visits included reviews of states' BCCP processes, but not their content
HHS/Low Income Housing Energy Assistance Program	As of July 2, a contractor had conducted on-site reviews of 20 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—on-site visits included reviews of states' BCCP processes, but not their content
HHS/Medicaid	A contractor conducted on-site reviews of 50 states and the District of Columbia once, and as of June 30, the contractor had conducted follow-up reviews of 14 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—Initial visits included a review of a state's BCCP process, and as of July 9, a contractor had reviewed the content of 42 states' BCCPs, either on site or at headquarters
HHS/ Temporary Assistance for Needy Families	As of July 2, a contractor had conducted on-site reviews of 20 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—on-site visits included reviews of states' BCCP processes, but not their content
Labor/ Unemployment Insurance	Labor's regional offices are monitoring all states' efforts	Unknown—not specifically addressed in methodology	Unknown—not specifically addressed in methodology	Reviews ongoing

In addition to the completed reviews, all of the departments have ongoing initiatives to ensure that state-administered human services programs will continue to function past the change of century. These initiatives are part of the departments' overall strategies to ensure the continued delivery of these high-impact programs. For example,

- In June 1999, the Department of Agriculture's FNS required its regions to provide for each program a copy of either a state letter certifying that it was Year 2000 compliant or a business continuity and contingency plan. As of June 18, 1999, FNS had received (1) 9 certifications and 7 business continuity and contingency plans for Child Nutrition; (2) 12 certifications and 16 business continuity and contingency plans for Food Stamps; and (3) 23 certifications and 23 business continuity and contingency plans for Women, Infants, and Children. In addition, to help states' Year 2000 efforts, FNS employed a contractor to conduct on-site visits to 20 states for one or more programs. As of July 9, FNS officials told us 16 states had been visited. With respect to the scope of these visits, FNS' regional offices determine for each state and program what specific areas it should encompass. These visits are principally intended to provide technical assistance to the states in areas such as Year 2000 project management, hardware and software testing, and contingency planning.

- In its initial round of on-site reviews conducted between November 1998 and April 1999, the contractor hired by HHS' HCFA (1) identified barriers to successful remediation; (2) made recommendations to address specific areas of concern; and (3) placed Medicaid integrated eligibility and management information systems into low, medium, or high risk categories. HCFA's contractor is currently conducting a second round of on-site reviews in at least 40 states—primarily those in which at least one of two systems was categorized as a high or medium risk during the initial visit. As of June 30, 14 states had been visited during this round. The focus of this second round of visits is on determining how states have resolved Year 2000 issues previously identified, as well as reviewing activities such as data exchanges and end-to-end testing. HCFA plans to conduct a third round of on-site reviews in the fall of 1999 for those states that continue to have systems categorized as high risk. Additionally, another HCFA contractor is reviewing the content of all states' business continuity and contingency plans, with some of these reviews being performed in conjunction with the second round of state visits.

- In September 1998, the Department of Labor required that all State Employment Security Agencies conduct independent verification and validation reviews of their Unemployment Insurance programs. The department set a target date of July 1, 1999, for states to submit independent verification and validation certifications of their Unemployment Insurance systems to Labor's regional offices. Labor required its regional offices to review independent verification and validation reports and certifications of Year 2000 compliance that State Employment Security Agencies submitted, and ascertain whether the material met the department's requirements. If Labor's requirements were met, the regional offices were to approve the State Employment Security Agencies' certification and independent verification and validation reports and forward copies of the approved certification and report, along

with regional office comments, to Labor's national office.

An example of the benefits that federal/state partnerships can provide is illustrated by the Department of Labor's unemployment services program. In September 1998, we reported that many State Employment Security Agencies were at risk of failure as early as January 1999 and urged the Department of Labor to initiate the development of realistic contingency plans to ensure continuity of core business processes in the event of Year 2000-induced failures.[52] In May, we testified that four state agencies' systems could have failed if systems in those states had not been programmed with an emergency patch in December 1998. This patch was developed by several of the state agencies and promoted to other state agencies by the Department of Labor.[53]

YEAR 2000 READINESS INFORMATION AVAILABLE IN SOME SECTORS, BUT KEY INFORMATION STILL MISSING OR INCOMPLETE

Beyond the risks faced by federal, state, and local governments, the year 2000 also poses a serious challenge to the public infrastructure, key economic sectors, and to other countries. To address these concerns, in April 1998 we recommended that the Council use a sector-based approach and establish the effective public-private partnerships necessary to address this issue.[54] The Council subsequently established over 25 sector-based working groups and has been initiating outreach activities since it became operational last spring. In addition, the Chair of the Council has formed a Senior Advisors Group composed of representatives from private-sector firms across key economic sectors. Members of this group are expected to offer perspectives on cross-cutting issues, information sharing, and appropriate federal responses to potential Year 2000 failures.

Our April 1998 report also recommended that the President's Council develop a comprehensive picture of the nation's Year 2000 readiness, to include identifying and assessing risks to the nation's key economic sectors—including risks posed by international links. In October 1998 the Chair directed the Council's sector working groups to begin assessing their sectors. The Chair also provided a recommended guide of core questions that the Council asked to be included in surveys by the associations performing the assessments. These questions included the percentage of work that has been completed in the assessment, renovation, validation, and implementation phases. The Chair then planned to issue quarterly public reports summarizing these assessments.

[52] Year 2000 Computing Crisis: Progress Made at Department of Labor, But Key Systems at Risk (GAO/T-AIMD-98-303, September 17, 1998).
[53] Year 2000 Computing Challenge: Labor Has Progressed But Selected Systems Remain at Risk (GAO/T-AIMD-99-179, May 12, 1999).
[54] GAO/AIMD-98-85, April 30, 1998.

The Council's most recent report was issued on August 5, 1999.[55] The report stated that important national systems will make a successful transition to the year 2000 but that much work, such as contingency planning, remains to be done. In particular, the Council expressed a high degree of confidence in five major domestic areas: financial institutions, electric power, telecommunications, air travel, and the federal government. For example, the Council stated that on August 2, federal bank, thrift, and credit union regulators reported that 99 percent of federally insured financial institutions have completed testing of critical systems for Year 2000 readiness. The Council had concerns in four significant areas: local government, health care, education, and small businesses. For example, according to the Council report, many school districts could move into the new century with dysfunctional information technology systems, since only 28 percent and 30 percent of Superintendent/Local Educational Agencies and post-secondary institutions, respectively, reported that their mission-critical systems were Year 2000 compliant. Internationally, the Council stated that the Year 2000 readiness of other countries was improving but was still a concern. The Council reported that the June 1999 meeting of National Year 2000 Coordinators held at the United Nations found that the 173 countries in attendance were clearly focused on the Year 2000 problem but that many countries will likely not have enough time or resources to finish before the end of 1999.

The Council's assessment reports have substantially increased the nation's understanding of the Year 2000 readiness of key industries. However, the picture remains incomplete in certain key areas because the surveys conducted to date did not have a high response rate or did not provide their response rate; the assessment was general or contained projections rather than current remediation information; or the data were old. For example, according to the Council's latest assessment report,

- Less than a quarter of the more than 16,000 Superintendents of Schools/Local Educational Agencies responded to a web-based survey of Year 2000 readiness among elementary and secondary schools. Similarly, less than a third of the more than 6,000 presidents and/or chancellors of post-secondary educational institutions responded to a web-based Year 2000 survey. Also, surveys covering areas such as small and medium-sized chemical enterprises did not provide information on either the number of surveys distributed or the number returned. Small response rates or the lack of information on response rates call into question whether the results of the survey accurately portray the readiness of the sector.

- Information in areas, such as state emergency management and broadcast television and radio provided a general assessment or projected compliance levels as of a certain date, but did not contain detailed data as to the current status of the sector (e.g., the average percentage of organizations' systems that are Year 2000 compliant or the

[55] The Council's three reports are available on its web site, *www.y2k.gov*. In addition, the Council, in conjunction with the Federal Trade Commission and the General Services Administration, has established a toll-free Year 2000 information line, 1-888-USA-4Y2K. The Federal Trade Commission has also included Year 2000 information of interest to consumers on its web site, *www.consumer.gov*.

percentage of organizations that are in the assessment, renovation, or validation phases).

- In some cases, such as for grocery manufacturers, cable television, hospitals, physicians' practices, and railroads, the sector surveys had been conducted months earlier and/or current survey information was not yet available.

In addition to our work related to the federal, state, and local government's Year 2000 progress, we have also issued several products related to key economic sectors. I will now discuss the results of these reviews.

Energy Sector

In April, we reported that while the electric power industry had concluded that it had made substantial progress in making its systems and equipment ready to continue operations into the year 2000, significant risks remained since many reporting organizations did not expect to be Year 2000 ready within the June 1999 industry target date.[56] We, therefore, suggested that the Department of Energy (1) work with the Electric Power Working Group to ensure that remediation activities were accelerated for the utilities that expected to miss the June 1999 deadline for achieving Year 2000 readiness and (2) encourage state regulatory utility commissions to require a full public disclosure of Year 2000 readiness status of entities transmitting and distributing electric power. The Department of Energy generally agreed with our suggestions. We also suggested that the Nuclear Regulatory Commission (1) in cooperation with the Nuclear Energy Institute, work with nuclear power plant licensees to accelerate the Year 2000 remediation efforts among the nuclear power plants that expect to meet the June 1999 deadline for achieving readiness and (2) publicly disclose the Year 2000 readiness of each of the nation's operational nuclear reactors. In response, the Nuclear Regulatory Commission stated that it plans to focus its efforts on nuclear power plants that may miss the July 1, 1999 milestone and that it would release the readiness information on individual plants that same month.

Subsequent to our report, on August 3, 1999, the North American Electric Reliability Council released its fourth status report on electric power systems. According to the Council, as of June 30, 1999—the industry target date for organizations to be Year 2000 ready—251 of 268 (94 percent) of bulk electric organizations were Year 2000 ready or Year 2000 ready with limited exceptions.[57] In addition, this report stated that 96 percent

[56] Year 2000 Computing Crisis: Readiness of the Electric Power Industry (GAO/AIMD-99-114, April 6, 1999).

[57] The North American Electric Reliability Council reported that 64 of these organizations had exceptions but that it "believes that the work schedule provided to complete these exception items in the next few months represents a prudent use of resources and does not increase risks associated with reliable electric service into the Year 2000."

of local distribution systems were reported as Year 2000 ready.[58] The North American Electric Reliability Council stated that the information it uses is principally self-reported but that 84 percent of the organizations reported that their Year 2000 programs had also been audited by internal and/or external auditors. On July 19, the Nuclear Regulatory Commission stated that 68 of 103 (66 percent) nuclear power plants reported that all of their computer systems and digital embedded components that support plant operations are Year 2000 ready. Of the 35 plants that were not Year 2000 ready, 18 had systems or components that were not ready that could affect power generation.

In May, we reported[59] that while the domestic oil and gas industries had reported that they had made substantial progress in making their equipment and systems ready to continue operations into the year 2000, risks remained. For example, although over half of our oil is imported, little was known about the Year 2000 readiness of foreign oil suppliers. Further, while individual domestic companies reported that they were developing Year 2000 contingency plans, there were no plans to perform a national-level risk assessment and develop contingency plans to deal with potential shortages or disruptions in the nation's overall oil and gas supplies. We suggested that the Council's oil and gas working group (1) work with industry associations to perform national-level risk assessments and develop and publish credible, national-level scenarios regarding the impact of potential Year 2000 failures and (2) develop national-level contingency plans. The working group generally agreed with these suggestions.

Water Sector

In April we reported[60] that insufficient information was available to assess and manage Year 2000 efforts in the water sector, and little additional information was expected under the current regulatory approach. While the Council's water sector working group had undertaken an awareness campaign and had urged national water sector associations to continue to survey their memberships, survey response rates had been low. Further, Environmental Protection Agency officials stated that the agency lacked the rules and regulations necessary to require water and wastewater facilities to report on their Year 2000 status.

Our survey of state regulators found that a few states were proactively collecting Year 2000 compliance data from regulated facilities, a much larger group of states was disseminating Year 2000 information, while another group was not actively using either approach. Additionally, only a handful of state regulators believed that they were

[58] This was based on the percentage of the total megawatts of the systems reported as Year 2000 ready by investor-owned, public power, and cooperative organizations. The report did not identify the number of local distribution organizations that reported that they were Year 2000 ready.

[59] Year 2000 Computing Crisis: Readiness of the Oil and Gas Industries (GAO/AIMD-99-162, May 19, 1999).

[60] Year 2000 Computing Crisis: Status of the Water Industry (GAO/AIMD-99-151, April 21, 1999).

responsible for ensuring facilities' Year 2000 compliance or overseeing facilities' business continuity and contingency plans. Among our suggested actions was that the Council, the Environmental Protection Agency, and the states determine which regulatory organization should take responsibility for assessing and publicly disclosing the status and outlook of water sector facilities' Year 2000 business continuity and contingency plans. The Environmental Protection Agency generally agreed with our suggestions but one official noted that additional legislation may be needed if the agency is to take responsibility for overseeing facilities' Year 2000 business continuity and contingency plans.

Health Sector

The health sector includes health care providers (such as hospitals and emergency health care services), insurers (such as Medicare and Medicaid), and biomedical equipment. Last month we reported[61] that HCFA had taken aggressive and comprehensive outreach efforts with regard to its over 1.1 million healthcare providers that administer services for Medicare-insured patients.[62] Despite these efforts, HCFA data show that provider participation in its outreach activities has been low. Further, although HCFA has tasked contractors that process Medicare claims with testing with providers using future-dated claims, such testing had been limited and the testing that had occurred had identified problems. Our July report also found that although many surveys had been completed in 1999 on the Year 2000 readiness of healthcare providers; none of the 11 surveys we reviewed provided sufficient information with which to assess the Year 2000 status of the healthcare provider community. Each of the surveys had low response rates, and several did not address critical questions about testing and contingency planning.

To reduce the risk of Year 2000-related failures in the Medicare provider community, our July report suggested, for example, that HCFA consider using additional outreach methods, such as public service announcements, and set milestones for Medicare contractors for testing with providers. We also made suggestions to the President's Council on Year 2000 Conversion's healthcare sector working group, including a suggestion to consider working with associations to publicize those providers who respond to future surveys in order to increase survey response rates. The HCFA Administrator generally agreed with our suggested actions.

With respect to biomedical equipment, on June 10 we testified[63] that, in response to our September 1998 recommendation, [64] HHS, in conjunction with the Department of

[61] Year 2000 Computer Crisis: Status of Medicare Providers Unknown (GAO/AIMD-99-243, July 28, 1999).

[62] Examples of such providers are hospitals, laboratories, physicians, and skilled nursing/long term care facilities.

[63] Year 2000 Computing Challenge: Concerns About Compliance Information on Biomedical Equipment (GAO/T-AIMD-99-209, June 10, 1999).

[64] Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown (GAO/AIMD-98-240, September 18, 1998).

Veterans Affairs, had established a clearinghouse on biomedical equipment. As of June 1, 1999, 4,142 biomedical equipment manufacturers had submitted data to the clearinghouse. About 61 percent of these manufacturers reported having products that do not employ dates and about 8 percent (311 manufacturers) reported having date-related problems such as an incorrect display of date/time. According to the Food and Drug Administration, the 311 manufacturers reported 897 products with date-related problems. However, not all compliance information was available on the clearinghouse because the clearinghouse referred the user to 427 manufacturers' web sites. Accordingly, we reviewed the web sites of these manufacturers and found, as of June 1, 1999, a total of 35,446 products.[65] Of these products, 18,466 were reported as not employing a date, 11,211 were reported as compliant, 4,445 were shown as not compliant, and the compliance status of 1,324 was unknown.

In addition to the establishment of a clearinghouse, our September 1998 report[66] also recommended that HHS and the Department of Veterans Affairs take prudent steps to jointly review manufacturers' test results for critical care/life support biomedical equipment. We were especially concerned that the departments review test results for equipment previously deemed to be noncompliant but now deemed by manufacturers to be compliant, or equipment for which concerns about compliance remained. In May 1999, the Food and Drug Administration, a component agency of HHS, announced that it planned to develop a list of critical care/life support medical devices and the manufacturers of these devices, select a sample of manufacturers for review, and hire a contractor to develop a program to assess manufacturers' activities to identify and correct Year 2000 problems for these medical devices. In addition, if the results of this review indicated a need for further review of manufacturer activities, the contractor would review a portion of the remaining manufacturers not yet reviewed. Moreover, according to the Food and Drug Administration, any manufacturer whose quality assurance system appeared deficient based on the contractors review would be subject to additional reviews to determine what actions would be required to eliminate any risk posed by noncompliant devices.

In April testimony[67] we also reported on the results of a Department of Veterans Affairs survey of 384 pharmaceutical firms and 459 medical-surgical firms with whom it does business. Of the 52 percent of pharmaceutical firms that responded to the survey, 32 percent reported that they were compliant. Of the 54 percent of the medical-surgical firms that responded, about two-thirds reported that they were compliant.

[65] Because of limitations in many of the manufacturers web sites, our ability to determine the total number of biomedical equipment products reported and their compliance status was impaired. Accordingly, the actual number of products reported by the manufacturers could be significantly higher than the 35,446 products that we counted.

[66] GAO/AIMD-98-240, September 18, 1998.

[67] Year 2000 Computing Crisis: Action Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/T-AIMD-99-136, April 15, 1999).

Banking and Finance Sector

A large portion of the institutions that make up the banking and finance sector are overseen by one or more federal regulatory agencies. In September 1998 we testified on the efforts of five federal financial regulatory agencies[68] to ensure that the institutions that they oversee are ready to handle the Year 2000 problem.[69] We concluded that the regulators had made significant progress in assessing the readiness of member institutions and in raising awareness on important issues such as contingency planning and testing. Regulator examinations of bank, thrift, and credit union Year 2000 efforts found that the vast majority were doing a satisfactory job of addressing the problem. Nevertheless, the regulators faced the challenge of ensuring that they are ready to take swift action to address those institutions that falter in the later stages of correction and to address disruptions caused by international and public infrastructure failures.

In April, we reported that the Federal Reserve System--which is instrumental to our nation's economic well-being, since it provides depository institutions and government agencies services such as processing checks and transferring funds and securities, has effective controls to help ensure that its Year 2000 progress is reported accurately and reliably.[70] We also found that it is effectively managing the renovation and testing of its internal systems and the development and planned testing of contingency plans for continuity of business operations. Nevertheless, the Federal Reserve System still had much to accomplish before it is fully ready for January 1, 2000, such as completing validation and implementation of all of its internal systems and completing its contingency plans.

In addition to the domestic banking and finance sector, large U.S. financial institutions have financial exposures and relationships with international financial institutions and markets that may be at risk if these international organizations are not ready for the date change occurring on January 1, 2000. In April, we reported[71] that foreign financial institutions had reportedly lagged behind their U.S. counterparts in preparing for the Year 2000 date change. Officials from four of the seven large foreign financial institutions we visited said they had scheduled completion of their Year 2000 preparations about 3 to 6 months after their U.S. counterparts, but they planned to complete their efforts by mid-1999 at the latest. Moreover, key international market supporters, such as those that transmit financial messages and provide clearing and settlement services, told us that

[68] The National Credit Union Administration, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Federal Reserve System, and the Office of the Comptroller of the Currency.

[69] Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain (GAO/T-AIMD-98-305, September 17, 1998).

[70] Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Conversion (GAO/AIMD-99-78, April 9, 1999).

[71] Year 2000: Financial Institution and Regulatory Efforts to Address International Risks (GAO/GGD-99-62, April 27, 1999).

their systems were ready for the date change and that they had begun testing with the financial organizations that depended on these systems. Further, we found that seven large U.S. banks and securities firms we visited were taking actions to address their international risks. In addition, U.S. banking and securities regulators were also addressing the international Year 2000 risks of the institutions that they oversee.

With respect to the insurance industry, in March, we concluded that insurance regulator presence regarding the Year 2000 area was not as strong as that exhibited by the banking and securities industry.[72] State insurance regulators we contacted were late in raising industry awareness of potential Year 2000 problems, provided little guidance to regulated institutions, and failed to convey clear regulatory expectations to companies about Year 2000 preparations and milestones. Nevertheless, the insurance industry is reported by both its regulators and by other outside observers to be generally on track to being ready for 2000. However, most of these reports are based on self-reported information and, compared to other financial regulators, insurance regulators' efforts to validate this information generally began late and were more limited.

In a related report in April,[73] we stated that variations in oversight approaches by state insurance regulators also made it difficult to ascertain the overall status of the insurance industry's Year 2000 readiness. We reported that the magnitude of insurers' Year 2000-related liability exposures could not be estimated at that time but that costs associated with these exposures could be substantial for some property-casualty insurers, particularly those concentrated in commercial-market sectors. In addition, despite efforts to mitigate potential exposures, the Year 2000-related costs that may be incurred by insurers would remain uncertain until key legal issues and actions on pending legislation were resolved.

Transportation Sector

A key component to the nation's transportation sector are airports. This January we reported on our survey of 413 airports.[74] We found that while the nation's airports were making progress in preparing for the year 2000, such progress varied. Of the 334 airports responding to our survey, about one-third reported that they would complete their Year 2000 preparations by June 30, 1999. The other two-thirds either planned on a later date or failed to estimate any completion date, and half of these airports did not have contingency plans for any of 14 core airport functions. Although most of those not expecting to be ready by June 30 are small airports, 26 of them are among the nation's largest 50 airports.

[72] Insurance Industry: Regulators Are Less Active in Encouraging and Validating Year 2000 Preparedness (GAO/T-GGD-99-56, March 11, 1999).

[73] Year 2000: State Insurance Regulators Face Challenges in Determining Industry Readiness (GAO/GGD-99-87, April 30, 1999).

[74] Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem (GAO/RCED/AIMD-99-57, January 29, 1999).

International

In addition to the risks associated with the nation's key economic sectors, one of the largest and most uncertain area of risk relates to the global nature of the problem. Table 3 summarizes the results of the Department of State's Office of the Inspector General's analysis of "Y2K Host Country Infrastructure" assessments submitted by U.S. embassies in 161 countries (98 from the developing world, 24 from former Easter bloc countries and the New Independent States, and 39 from industrialized countries). The following table shows that about half of the countries are reported to be at medium or high risk of having Year 2000-related failures in the key areas of telecommunications, transportation, and energy. While a smaller number of countries were reported at medium or high risk in the finance and water sectors, at least one third of the countries fell into the medium or high risk categories.

Table 3: Risk of Year 2000-Related Sector Failures in 161 Countries

Risk Level	Finance	Telecommunications	Transportation	Energy	Water
High	11	35	18	26	7
Medium	43	56	61	64	52
Low	107	70	82	71	102

Source: Year 2000 Computer Problem: Global Readiness and International Trade (Statement of the Department of State's Inspector General before the Senate Special Committee on the Year 2000 Technology Problem, July 22, 1999).

The Department of State Inspector General concluded that the global community is likely to experience varying degrees of Year 2000-related failures—from mere annoyances to failures in key infrastructure systems—in every sector, region, and economic level. In particular, the Inspector General testified on July 22, 1999, that

- Industrialized countries were generally at low risk of having Year 2000-related infrastructure failures although some of these countries were at risk.

- Developing countries were lagging behind and were struggling to find the financial and technical resources needed to resolve their Year 2000 problems.

- Former Eastern bloc countries were late in getting started and were generally unable to provide detailed information on their Year 2000 programs.

The impact of Year 2000-induced failures in foreign countries could adversely affect the United States, particularly as it relates to the supply chain. To address the international supply chain issue, in January 1999 we suggested[75] that the President's Council on Year

[75] GAO/T-AIMD-99-50, January 20, 1999.

2000 Conversion prioritize trade and commerce activities that are critical to the nation's well-being (e.g., oil, food, pharmaceuticals) and, working with the private sector, identify options for obtaining these materials through alternative avenues in the event that Year 2000-induced failures in the other country or in the transportation sector prevent these items from reaching the United States. In commenting on this suggestion, the Chair stated that the Council had (1) worked with federal agencies to identify sectors with the greatest dependence on international trade, (2) held industry roundtable discussions with the pharmaceutical and food supply sectors, and (3) hosted bilateral and trilateral meetings with the Council's counterparts in Canada and Mexico—the United States' largest trading partners.

- - - - -

In summary, while improvement has been shown, much work remains at the national, federal, state, and local levels to ensure that major service disruptions do not occur. Specifically, remediation must be completed, end-to-end testing performed, and business continuity and contingency plans developed. Similar actions remain to be completed by the nation's key sectors. Accordingly, whether the United States successfully confronts the Year 2000 challenge will largely depend on the success of federal, state, and local governments, as well as the private sector working separately and together to complete these actions. Accordingly, strong leadership and partnerships must be maintained to ensure that the needs of the public are met at the turn of the century.

Mr. Chairman, this concludes my statement. I would be happy to respond to any questions that you or other members of the Subcommittee may have at this time.

Contacts

For information concerning this testimony, please contact Joel Willemssen at (202) 512-6253 or by e-mail at willemssenj.aimd@gao.gov.

Federal High-Impact Programs and Lead Agencies

Agency	Program
Department of Agriculture	Child Nutrition Programs
Department of Agriculture	Food Safety Inspection
Department of Agriculture	Food Stamps
Department of Agriculture	Special Supplemental Nutrition Program for Women, Infants, and Children
Department of Commerce	Patent and trademark processing
Department of Commerce	Weather Service
Department of Defense	Military Hospitals
Department of Defense	Military Retirement
Department of Education	Student Aid
Department of Energy	Federal electric power generation and delivery
Department of Health and Human Services	Child Care
Department of Health and Human Services	Child Support Enforcement
Department of Health and Human Services	Child Welfare
Department of Health and Human Services	Disease monitoring and the ability to issue warnings
Department of Health and Human Services	Indian Health Service
Department of Health and Human Services	Low Income Home Energy Assistance Program
Department of Health and Human Services	Medicaid
Department of Health and Human Services	Medicare
Department of Health and Human Services	Organ Transplants
Department of Health and Human Services	Temporary Assistance for Needy Families
Department of Housing and Urban Development	Housing loans (Government National Mortgage Association)

Department of Housing and Urban Development	Section 8 Rental Assistance
Department of Housing and Urban Development	Public Housing
Department of Housing and Urban Development	FHA Mortgage Insurance
Department of Housing and Urban Development	Community Development Block Grants
Department of the Interior	Bureau of Indians Affairs programs
Department of Justice	Federal Prisons
Department of Justice	Immigration
Department of Justice	National Crime Information Center
Department of Labor	Unemployment Insurance
Department of State	Passport Applications and Processing
Department of Transportation	Air Traffic Control System
Department of Transportation	Maritime Safety Program
Department of the Treasury	Cross-border Inspection Services
Department of Veterans Affairs	Veterans' Benefits
Department of Veterans Affairs	Veterans' Health Care
Federal Emergency Management Agency	Disaster Relief
Office of Personnel Management	Federal Employee Health Benefits
Office of Personnel Management	Federal Employee Life Insurance
Office of Personnel Management	Federal Employee Retirement Benefits
Railroad Retirement Board	Retired Rail Workers Benefits
Social Security Administration	Social Security Benefits
U.S. Postal Service	Mail Service

GAO REPORTS AND TESTIMONY ADDRESSING THE YEAR 2000 CRISIS

Year 2000 Computing Challenge: Agencies' Reporting of Mission-Critical Classified Systems (GAO/AIMD-99-218, August 5, 1999)

Social Security Administration: Update on Year 2000 and Other Key Information Technology Initiatives (GAO/T-AIMD-99-259, July 29, 1999)

Year 2000 Computing Crisis: Status of Medicare Providers Unknown (GAO/AIMD-99-243, July 28, 1999)

Reported Y2K status of the 21 Largest U.S. Cities (GAO/AIMD-99-246R, July 15, 1999)

Year 2000 Computing Challenge: Federal Efforts to Ensure Continued Delivery of Key State-Administered Benefits (GAO/T-AIMD-99-241, July 15, 1999)

Emergency and State and Local Law Enforcement Systems: Committee Questions Concerning Year 2000 Challenges (GAO/AIMD-99-247R, July 14, 1999)

Year 2000 Computing Challenge: Important Progress Made, Yet Much Work Remains to Avoid Disruption of Critical Services (GAO/T-AIMD-99-234, July 9, 1999)

Year 2000 Computing Challenge: Readiness Improving Yet Avoiding Disruption of Critical Services Will Require Additional Work (GAO/T-AIMD-99-233, July 8, 1999)

Year 2000 Computing Challenge: Readiness Improving But Much Work Remains to Avoid Disruption of Critical Services (GAO/T-AIMD-99-232, July 7, 1999)

Defense Computers: Management Controls Are Critical To Effective Year 2000 Testing (GAO/AIMD-99-172, June 30, 1999)

Year 2000 Computing Crisis: Customs is Making Good Progress (GAO/T-AIMD-99-225, June 29, 1999)

Year 2000 Computing Challenge: Delivery of Key Benefits Hinges on States' Achieving Compliance (GAO/T-AIMD/GGD-99-221, June 23, 1999)

Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications (GAO/T-AIMD-99-214, June 22, 1999).

GSA's Effort to Develop Year 2000 Business Continuity and Contingency Plans for Telecommunications Systems (GAO/AIMD-99-201R, June 16, 1999).

Year 2000 Computing Crisis: Actions Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/AIMD-99-190R, June 11, 1999)

Year 2000 Computing Challenge: Concerns About Compliance Information on Biomedical Equipment (GAO/T-AIMD-99-209, June 10, 1999)

Year 2000 Computing Challenge: Much Biomedical Equipment Status Information Available, Yet Concerns Remain (GAO/T-AIMD-99-197, May 25, 1999)

Year 2000 Computing Challenge: OPM Has Made Progress on Business Continuity Planning (GAO/GGD-99-66, May 24, 1999)

VA Y2K Challenges: Responses to Post-Testimony Questions (GAO/AIMD-99-199R, May 24, 1999)

Year 2000 Computing Crisis: USDA Needs to Accelerate Time Frames for Completing Contingency Planning (GAO/AIMD-99-178, May 21, 1999)

Year 2000 Computing Crisis: Readiness of the Oil and Gas Industries (GAO/AIMD-99-162, May 19, 1999)

Year 2000 Computing Challenge: Time Issues Affecting the Global Positioning System (GAO/T-AIMD-99-187, May 12, 1999)

Year 2000 Computing Challenge: Education Taking Needed Actions But Work Remains (GAO/T-AIMD-99-180, May 12, 1999)

Year 2000 Computing Challenge: Labor Has Progressed But Selected Systems Remain at Risk (GAO/T-AIMD-99-179, May 12, 1999)

Year 2000: State Insurance Regulators Face Challenges in Determining Industry Readiness (GAO/GGD-99-87, April 30, 1999)

Year 2000 Computing Challenge: Status of Emergency and State and Local Law Enforcement Systems Is Still Unknown (GAO/T-AIMD-99-163, April 29, 1999)

Year 2000 Computing Crisis: Costs and Planned Use of Emergency Funds (GAO/AIMD-99-154, April 28, 1999)

Year 2000: Financial Institution and Regulatory Efforts to Address International Risks (GAO/GGD-99-62, April 27, 1999)

Year 2000 Computing Crisis: Readiness of Medicare and the Health Care Sector (GAO/T-AIMD-99-160, April 27, 1999)

U.S. Postal Service: Subcommittee Questions Concerning Year 2000 Challenges Facing the Service (GAO/AIMD-99-150R, April 23, 1999)

Year 2000 Computing Crisis: Status of the Water Industry (GAO/AIMD-99-151, April 21, 1999)

Year 2000 Computing Crisis: Key Actions Remain to Ensure Delivery of Veterans Benefits and Health Services (GAO/T-AIMD-99-152, April 20, 1999)

Year 2000 Computing Crisis: Readiness Improving But Much Work Remains To Ensure Delivery of Critical Services (GAO/T-AIMD-99-149, April 19, 1999)

Year 2000 Computing Crisis: Action Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/T-AIMD-99-136, April 15, 1999)

Year 2000 Computing Challenge: Federal Government Making Progress But Critical Issues Must Still Be Addressed to Minimize Disruptions (GAO/T-AIMD-99-144, April 14, 1999)

Year 2000 Computing Crisis: Additional Work Remains to Ensure Delivery of Critical Services (GAO/T-AIMD-99-143, April 13, 1999)

Tax Administration: IRS' Fiscal Year 2000 Budget Request and 1999 Tax Filing Season (GAO/T-GGD/AIMD-99-140, April 13, 1999).

Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Conversion (GAO/AIMD-99-78, April 9, 1999)

Year 2000 Computing Crisis: Readiness of the Electric Power Industry (GAO/AIMD-99-114, April 6, 1999)

Year 2000 Computing Crisis: Customs Has Established Effective Year 2000 Program Controls (GAO/AIMD-99-37, March 29, 1999)

Year 2000 Computing Crisis: FAA Is Making Progress But Important Challenges Remain (GAO/T-AIMD/RCED-99-118, March 15, 1999)

Insurance Industry: Regulators Are Less Active in Encouraging and Validating Year 2000 Preparedness (GAO/T-GGD-99-56, March 11, 1999)

Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed (GAO/T-AIMD-99-101, March 2, 1999)

Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services (GAO/T-AIMD-99-92, February 26, 1999)

Defense Information Management: Continuing Implementation Challenges Highlight the Need for Improvement (GAO/T-AIMD-99-93, February 25, 1999)

IRS' Year 2000 Efforts: Status and Remaining Challenges (GAO/T-GGD-99-35, February 24, 1999)

Department of Commerce: National Weather Service Modernization and NOAA Fleet Issues (GAO/T-AIMD/GGD-99-97, February 24, 1999)

Year 2000 Computing Crisis: Medicare and the Delivery of Health Services Are at Risk (GAO/T-AIMD-99-89, February 24, 1999)

Year 2000 Computing Crisis: Readiness of State Automated Systems That Support Federal Human Services Programs (GAO/T-AIMD-99-91, February 24, 1999)

Year 2000 Computing Crisis: Customs Is Effectively Managing Its Year 2000 Program (GAO/T-AIMD-99-85, February 24, 1999)

Year 2000 Computing Crisis: Update on the Readiness of the Social Security Administration (GAO/T-AIMD-99-90, February 24, 1999)

Year 2000 Computing Crisis: Challenges Still Facing the U.S. Postal Service (GAO/T-AIMD-99-86, February 23, 1999)

Year 2000 Computing Crisis: The District of Columbia Remains Behind Schedule (GAO/T-AIMD-99-84, February 19, 1999)

High-Risk Series: An Update (GAO/HR-99-1, January 1999)

Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem (GAO/RCED/AIMD-99-57, January 29, 1999)

Defense Computers: DOD's Plan for Execution of Simulated Year 2000 Exercises (GAO/AIMD-99-52R, January 29, 1999)

Year 2000 Computing Crisis: Status of Bureau of Prisons' Year 2000 Efforts (GAO/AIMD-99-23, January 27, 1999)

Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, January 20, 1999)

Year 2000 Computing Challenge: Readiness Improving, But Critical Risks Remain (GAO/T-AIMD-99-49, January 20, 1999)

Status Information: FAA's Year 2000 Business Continuity and Contingency Planning Efforts Are Ongoing (GAO/AIMD-99-40R, December 4, 1998)

Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, November 1998)

Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998)

Year 2000 Computing Crisis: Status of Efforts to Deal With Personnel Issues (GAO/AIMD/GGD-99-14, October 22, 1998)

Year 2000 Computing Crisis: Updated Status of Department of Education's Information Systems (GAO/T-AIMD-99-8, October 8, 1998)

Year 2000 Computing Crisis: The District of Columbia Faces Tremendous Challenges in Ensuring That Vital Services Are Not Disrupted (GAO/T-AIMD-99-4, October 2, 1998)

Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy (GAO/AIMD-98-284, September 28, 1998)

Year 2000 Computing Crisis: Leadership Needed to Collect and Disseminate Critical Biomedical Equipment Information (GAO/T-AIMD-98-310, September 24, 1998)

Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown (GAO/AIMD-98-240, September 18, 1998)

Year 2000 Computing Crisis: Significant Risks Remain to Department of Education's Student Financial Aid Systems (GAO/T-AIMD-98-302, September 17, 1998)

Year 2000 Computing Crisis: Progress Made at Department of Labor, But Key Systems at Risk (GAO/T-AIMD-98-303, September 17, 1998)

Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain (GAO/T-AIMD-98-305, September 17, 1998)

Year 2000 Computing Crisis: Federal Reserve Is Acting to Ensure Financial Institutions Are Fixing Systems But Challenges Remain (GAO/AIMD-98-248, September 17, 1998)

Responses to Questions on FAA's Computer Security and Year 2000 Program (GAO/AIMD-98-301R, September 14, 1998)

Year 2000 Computing Crisis: Severity of Problem Calls for Strong Leadership and Effective Partnerships (GAO/T-AIMD-98-278, September 3, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Partnerships Needed to Reduce Likelihood of Adverse Impact (GAO/T-AIMD-98-277, September 2, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Partnerships Needed to Mitigate Risks (GAO/T-AIMD-98-276, September 1, 1998)

Year 2000 Computing Crisis: State Department Needs To Make Fundamental Improvements To Its Year 2000 Program (GAO/AIMD-98-162, August 28, 1998)

Year 2000 Computing: EFT 99 Is Not Expected to Affect Year 2000 Remediation Efforts (GAO/AIMD-98-272R, August 28, 1998)

Year 2000 Computing Crisis: Progress Made in Compliance of VA Systems, But Concerns Remain (GAO/AIMD-98-237, August 21, 1998)

Year 2000 Computing Crisis: Avoiding Major Disruptions Will Require Strong Leadership and Effective Partnerships (GAO/T-AIMD-98-267, August 19, 1998)

Year 2000 Computing Crisis: Strong Leadership and Partnerships Needed to Address Risk of Major Disruptions (GAO/T-AIMD-98-266, August 17, 1998)

Year 2000 Computing Crisis: Strong Leadership and Partnerships Needed to Mitigate Risk of Major Disruptions (GAO/T-AIMD-98-262, August 13, 1998)

FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998)

Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, August 1998)

Internal Revenue Service: Impact of the IRS Restructuring and Reform Act on Year 2000 Efforts (GAO/GGD-98-158R, August 4, 1998)

Social Security Administration: Subcommittee Questions Concerning Information Technology Challenges Facing the Commissioner (GAO/AIMD-98-235R, July 10, 1998)

Year 2000 Computing Crisis: Actions Needed on Electronic Data Exchanges (GAO/AIMD-98-124, July 1, 1998)

Defense Computers: Year 2000 Computer Problems Put Navy Operations At Risk (GAO/AIMD-98-150, June 30, 1998)

Year 2000 Computing Crisis: Testing and Other Challenges Confronting Federal Agencies (GAO/T-AIMD-98-218, June 22, 1998)

Year 2000 Computing Crisis: Telecommunications Readiness Critical, Yet Overall Status Largely Unknown (GAO/T-AIMD-98-212, June 16, 1998)

GAO Views on Year 2000 Testing Metrics (GAO/AIMD-98-217R, June 16, 1998)

IRS' Year 2000 Efforts: Business Continuity Planning Needed for Potential Year 2000 System Failures (GAO/GGD-98-138, June 15, 1998)

Year 2000 Computing Crisis: Actions Must Be Taken Now to Address Slow Pace of Federal Progress (GAO/T-AIMD-98-205, June 10, 1998)

Defense Computers: Army Needs to Greatly Strengthen Its Year 2000 Program (GAO/AIMD-98-53, May 29, 1998)

Year 2000 Computing Crisis: USDA Faces Tremendous Challenges in Ensuring That Vital Public Services Are Not Disrupted (GAO/T-AIMD-98-167, May 14, 1998)

Securities Pricing: Actions Needed for Conversion to Decimals (GAO/T-GGD-98-121, May 8, 1998)

Year 2000 Computing Crisis: Continuing Risks of Disruption to Social Security, Medicare, and Treasury Programs (GAO/T-AIMD-98-161, May 7, 1998)

IRS' Year 2000 Efforts: Status and Risks (GAO/T-GGD-98-123, May 7, 1998)

Air Traffic Control: FAA Plans to Replace Its Host Computer System Because Future Availability Cannot Be Assured (GAO/AIMD-98-138R, May 1, 1998)

Year 2000 Computing Crisis: Potential For Widespread Disruption Calls For Strong Leadership and Partnerships (GAO/AIMD-98-85, April 30, 1998)

Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998)

Department of the Interior: Year 2000 Computing Crisis Presents Risk of Disruption to Key Operations (GAO/T-AIMD-98-149, April 22, 1998)

Tax Administration: IRS' Fiscal Year 1999 Budget Request and Fiscal Year 1998 Filing Season (GAO/T-GGD/AIMD-98-114, March 31, 1998)

Year 2000 Computing Crisis: Strong Leadership Needed to Avoid Disruption of Essential Services (GAO/T-AIMD-98-117, March 24, 1998)

Year 2000 Computing Crisis: Federal Regulatory Efforts to Ensure Financial Institution Systems Are Year 2000 Compliant (GAO/T-AIMD-98-116, March 24, 1998)

Year 2000 Computing Crisis: Office of Thrift Supervision's Efforts to Ensure Thrift Systems Are Year 2000 Compliant (GAO/T-AIMD-98-102, March 18, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Public/Private Cooperation Needed to Avoid Major Disruptions (GAO/T-AIMD-98-101, March 18, 1998)

Post-Hearing Questions on the Federal Deposit Insurance Corporation's Year 2000 (Y2K) Preparedness (AIMD-98-108R, March 18, 1998)

SEC Year 2000 Report: Future Reports Could Provide More Detailed Information (GAO/GGD/AIMD-98-51, March 6, 1998)

Year 2000 Readiness: NRC's Proposed Approach Regarding Nuclear Powerplants (GAO/AIMD-98-90R, March 6, 1998)

Year 2000 Computing Crisis: Federal Deposit Insurance Corporation's Efforts to Ensure Bank Systems Are Year 2000 Compliant (GAO/T-AIMD-98-73, February 10, 1998)

Year 2000 Computing Crisis: FAA Must Act Quickly to Prevent Systems Failures (GAO/T-AIMD-98-63, February 4, 1998)

FAA Computer Systems: Limited Progress on Year 2000 Issue Increases Risk Dramatically (GAO/AIMD-98-45, January 30, 1998)

Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998)

Year 2000 Computing Crisis: Actions Needed to Address Credit Union Systems' Year 2000 Problem (GAO/AIMD-98-48, January 7, 1998)

Veterans Health Administration Facility Systems: Some Progress Made In Ensuring Year 2000 Compliance, But Challenges Remain (GAO/AIMD-98-31R, November 7, 1997)

Year 2000 Computing Crisis: National Credit Union Administration's Efforts to Ensure Credit Union Systems Are Year 2000 Compliant (GAO/T-AIMD-98-20, October 22, 1997)

Social Security Administration: Significant Progress Made in Year 2000 Effort, But Key Risks Remain (GAO/AIMD-98-6, October 22, 1997)

Defense Computers: Technical Support Is Key to Naval Supply Year 2000 Success (GAO/AIMD-98-7R, October 21, 1997)

Defense Computers: LSSC Needs to Confront Significant Year 2000 Issues (GAO/AIMD-97-149, September 26, 1997)

Veterans Affairs Computer Systems: Action Underway Yet Much Work Remains To Resolve Year 2000 Crisis (GAO/T-AIMD-97-174, September 25, 1997)

Year 2000 Computing Crisis: Success Depends Upon Strong Management and Structured Approach, (GAO/T-AIMD-97-173, September 25, 1997)

Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997)

Defense Computers: SSG Needs to Sustain Year 2000 Progress (GAO/AIMD-97-120R, August 19, 1997)

Defense Computers: Improvements to DOD Systems Inventory Needed for Year 2000 Effort (GAO/AIMD-97-112, August 13, 1997)

Defense Computers: Issues Confronting DLA in Addressing Year 2000 Problems (GAO/AIMD-97-106, August 12, 1997)

Defense Computers: DFAS Faces Challenges in Solving the Year 2000 Problem (GAO/AIMD-97-117, August 11, 1997)

Year 2000 Computing Crisis: Time is Running Out for Federal Agencies to Prepare for the New Millennium (GAO/T-AIMD-97-129, July 10, 1997)

Veterans Benefits Computer Systems: Uninterrupted Delivery of Benefits Depends on Timely Correction of Year-2000 Problems (GAO/T-AIMD-97-114, June 26, 1997)

Veterans Benefits Computer Systems: Risks of VBA's Year-2000 Efforts (GAO/AIMD-97-79, May 30, 1997)

Medicare Transaction System: Success Depends Upon Correcting Critical Managerial and Technical Weaknesses (GAO/AIMD-97-78, May 16, 1997)

Medicare Transaction System: Serious Managerial and Technical Weaknesses Threaten Modernization (GAO/T-AIMD-97-91, May 16, 1997)

Year 2000 Computing Crisis: Risk of Serious Disruption to Essential Government Functions Calls for Agency Action Now (GAO/T-AIMD-97-52, February 27, 1997)

Year 2000 Computing Crisis: Strong Leadership Today Needed To Prevent Future Disruption of Government Services (GAO/T-AIMD-97-51, February 24, 1997)

High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997)

Mr. OSE. We're going to go through the other witnesses and then come back for questions. I actually think there are microphones on the table here in the event you want to sit to give your testimony. You're welcome to stand, of course.

Mr. Cordiner, from the State Auditor's Office.

Mr. CORDINER. Mr. Chairman, Congressman, and Members, I appreciate the opportunity to speak to you this morning on a very important topic. Thus far our office has had two opportunities to review the Y2K effort in California. The first of our audits was published in August 1998. Under the former administration, agencies self-reported their progress on remediating their systems to the Department of Information Technology, and we were concerned that those reportings were accurate reportings. So we looked at several of the systems of these agencies and found that they were overly optimistic as to where they currently were in their progress. In addition, we did some survey work and found the same held true for some other agencies.

Moreover, there were many of these agencies that had not begun to do business continuity planning, which we felt was critical in light of the fact that they would seem to be lagging behind on the remediation progress. Most were doing planning, but it was more of a disaster recovery type of planning rather than concentrating on what would happen if their remediation efforts failed or weren't done in time.

Based on our recommendations in the first audit, the legislature again wanted us to look at this area, and we did publish another report in February 1999. This time we looked—we chose a sample of what we considered the most critical agencies supplying services to Californians, and that would include health and safety, payment systems, and revenue agencies. We chose a sample of 14 agencies to look at. We looked at the critical systems supporting those programs and found that 11 of the 14 agencies had not completed their remediation of critical systems that by a previous administration Executive order should have been done by December 31, 1998.

Areas that weren't finished included thoroughly testing their systems, dealing with the threats posed by imbedded technology that those systems depend on, as well as data exchange partners. They hadn't fully agreed on formats or some hadn't tested that agreed-upon format to ensure that information passed between the data exchange partners would be seamless and wouldn't cause a corruption of data.

We also found that one of the State's two large data centers that many agencies depend on to support their systems didn't have—it had a risky strategy for Y2K in that the infrastructure that these other agencies depend on hadn't been thoroughly tested to determine that it would work. And they also had noncompliant products out there that they had notified others that they shouldn't use, but they hadn't removed them as we felt would be prudent in the circumstance.

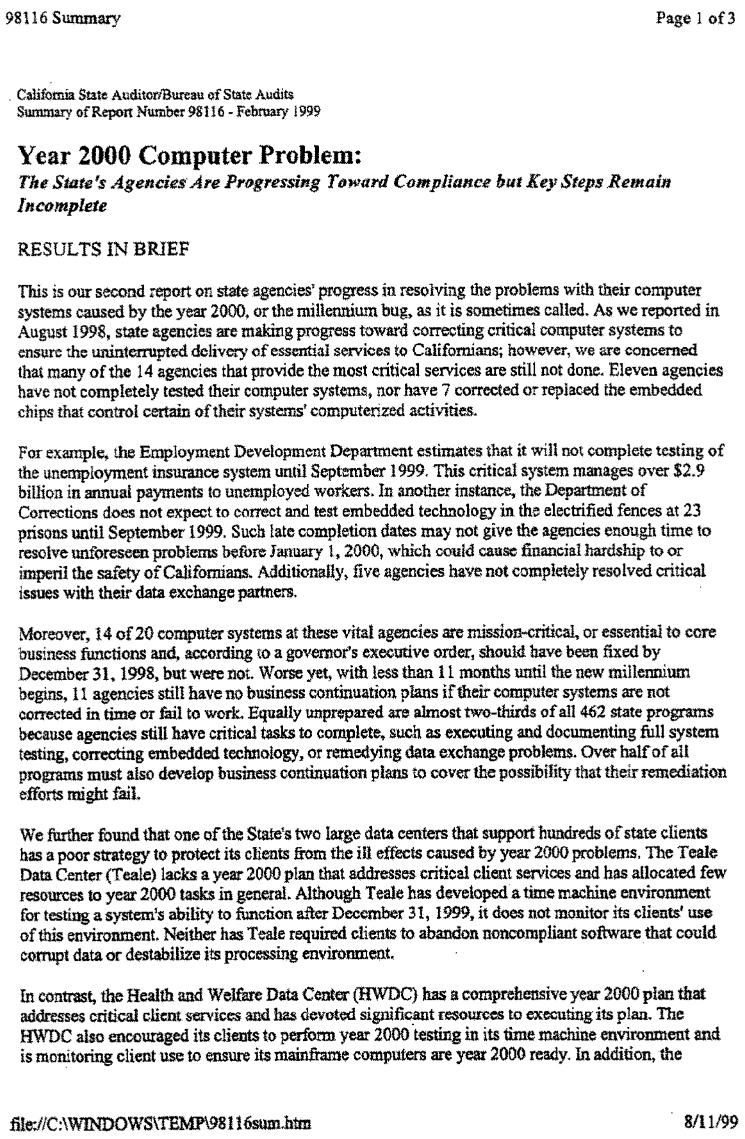
Last, we looked at the infrastructure, mainly telecommunications and the power grid, and we found that with the decentralization that has occurred in this industry, there are many players, if you will, that oversee segments of the infrastructure, but there was no centralized place that one could go to determine, you know, what's the progress on, say, telecommunications, or what's the progress on whether all the providers of power are fully ready to meet the new century.

That concludes my summary, and I would be glad to answer any questions.

Mr. OSE. We appreciate that. We're going to go ahead and have the other two testify and then we'll just take questions as a whole.

Mr. CORDINER. Thank you.

[The prepared statement of Mr. Cordiner follows:]



California State Auditor/Bureau of State Audits
Summary of Report Number 98116 - February 1999

Year 2000 Computer Problem:

The State's Agencies Are Progressing Toward Compliance but Key Steps Remain Incomplete

RESULTS IN BRIEF

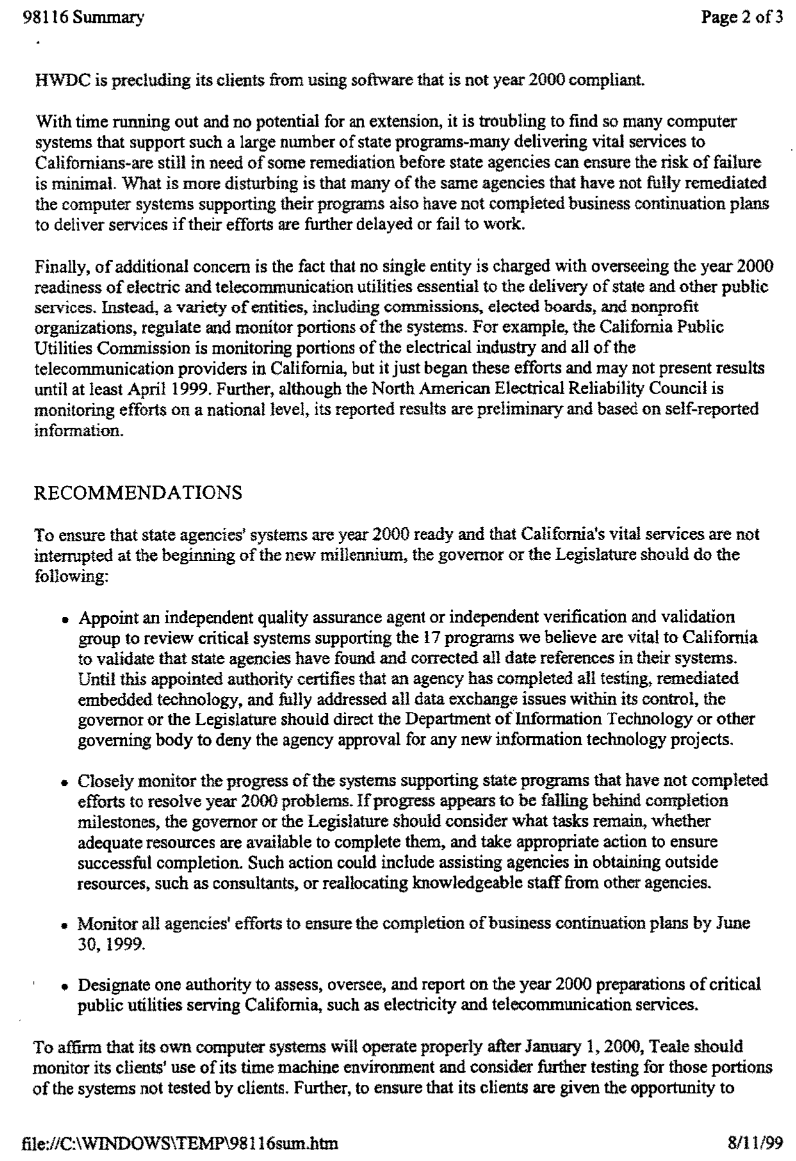
This is our second report on state agencies' progress in resolving the problems with their computer systems caused by the year 2000, or the millennium bug, as it is sometimes called. As we reported in August 1998, state agencies are making progress toward correcting critical computer systems to ensure the uninterrupted delivery of essential services to Californians; however, we are concerned that many of the 14 agencies that provide the most critical services are still not done. Eleven agencies have not completely tested their computer systems, nor have 7 corrected or replaced the embedded chips that control certain of their systems' computerized activities.

For example, the Employment Development Department estimates that it will not complete testing of the unemployment insurance system until September 1999. This critical system manages over $2.9 billion in annual payments to unemployed workers. In another instance, the Department of Corrections does not expect to correct and test embedded technology in the electrified fences at 23 prisons until September 1999. Such late completion dates may not give the agencies enough time to resolve unforeseen problems before January 1, 2000, which could cause financial hardship to or imperil the safety of Californians. Additionally, five agencies have not completely resolved critical issues with their data exchange partners.

Moreover, 14 of 20 computer systems at these vital agencies are mission-critical, or essential to core business functions and, according to a governor's executive order, should have been fixed by December 31, 1998, but were not. Worse yet, with less than 11 months until the new millennium begins, 11 agencies still have no business continuation plans if their computer systems are not corrected in time or fail to work. Equally unprepared are almost two-thirds of all 462 state programs because agencies still have critical tasks to complete, such as executing and documenting full system testing, correcting embedded technology, or remedying data exchange problems. Over half of all programs must also develop business continuation plans to cover the possibility that their remediation efforts might fail.

We further found that one of the State's two large data centers that support hundreds of state clients has a poor strategy to protect its clients from the ill effects caused by year 2000 problems. The Teale Data Center (Teale) lacks a year 2000 plan that addresses critical client services and has allocated few resources to year 2000 tasks in general. Although Teale has developed a time machine environment for testing a system's ability to function after December 31, 1999, it does not monitor its clients' use of this environment. Neither has Teale required clients to abandon noncompliant software that could corrupt data or destabilize its processing environment.

In contrast, the Health and Welfare Data Center (HWDC) has a comprehensive year 2000 plan that addresses critical client services and has devoted significant resources to executing its plan. The HWDC also encouraged its clients to perform year 2000 testing in its time machine environment and is monitoring client use to ensure its mainframe computers are year 2000 ready. In addition, the



HWDC is precluding its clients from using software that is not year 2000 compliant.

With time running out and no potential for an extension, it is troubling to find so many computer systems that support such a large number of state programs-many delivering vital services to Californians-are still in need of some remediation before state agencies can ensure the risk of failure is minimal. What is more disturbing is that many of the same agencies that have not fully remediated the computer systems supporting their programs also have not completed business continuation plans to deliver services if their efforts are further delayed or fail to work.

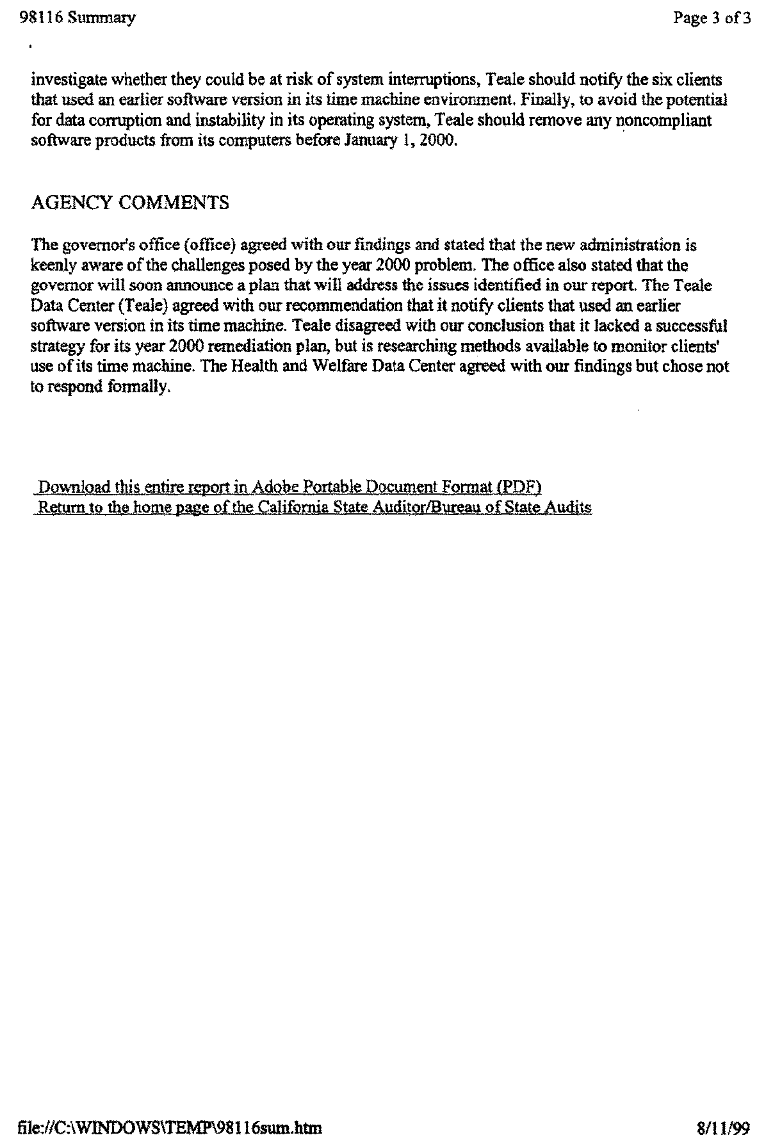
Finally, of additional concern is the fact that no single entity is charged with overseeing the year 2000 readiness of electric and telecommunication utilities essential to the delivery of state and other public services. Instead, a variety of entities, including commissions, elected boards, and nonprofit organizations, regulate and monitor portions of the systems. For example, the California Public Utilities Commission is monitoring portions of the electrical industry and all of the telecommunication providers in California, but it just began these efforts and may not present results until at least April 1999. Further, although the North American Electrical Reliability Council is monitoring efforts on a national level, its reported results are preliminary and based on self-reported information.

RECOMMENDATIONS

To ensure that state agencies' systems are year 2000 ready and that California's vital services are not interrupted at the beginning of the new millennium, the governor or the Legislature should do the following:

- Appoint an independent quality assurance agent or independent verification and validation group to review critical systems supporting the 17 programs we believe are vital to California to validate that state agencies have found and corrected all date references in their systems. Until this appointed authority certifies that an agency has completed all testing, remediated embedded technology, and fully addressed all data exchange issues within its control, the governor or the Legislature should direct the Department of Information Technology or other governing body to deny the agency approval for any new information technology projects.
- Closely monitor the progress of the systems supporting state programs that have not completed efforts to resolve year 2000 problems. If progress appears to be falling behind completion milestones, the governor or the Legislature should consider what tasks remain, whether adequate resources are available to complete them, and take appropriate action to ensure successful completion. Such action could include assisting agencies in obtaining outside resources, such as consultants, or reallocating knowledgeable staff from other agencies.
- Monitor all agencies' efforts to ensure the completion of business continuation plans by June 30, 1999.
- Designate one authority to assess, oversee, and report on the year 2000 preparations of critical public utilities serving California, such as electricity and telecommunication services.

To affirm that its own computer systems will operate properly after January 1, 2000, Teale should monitor its clients' use of its time machine environment and consider further testing for those portions of the systems not tested by clients. Further, to ensure that its clients are given the opportunity to

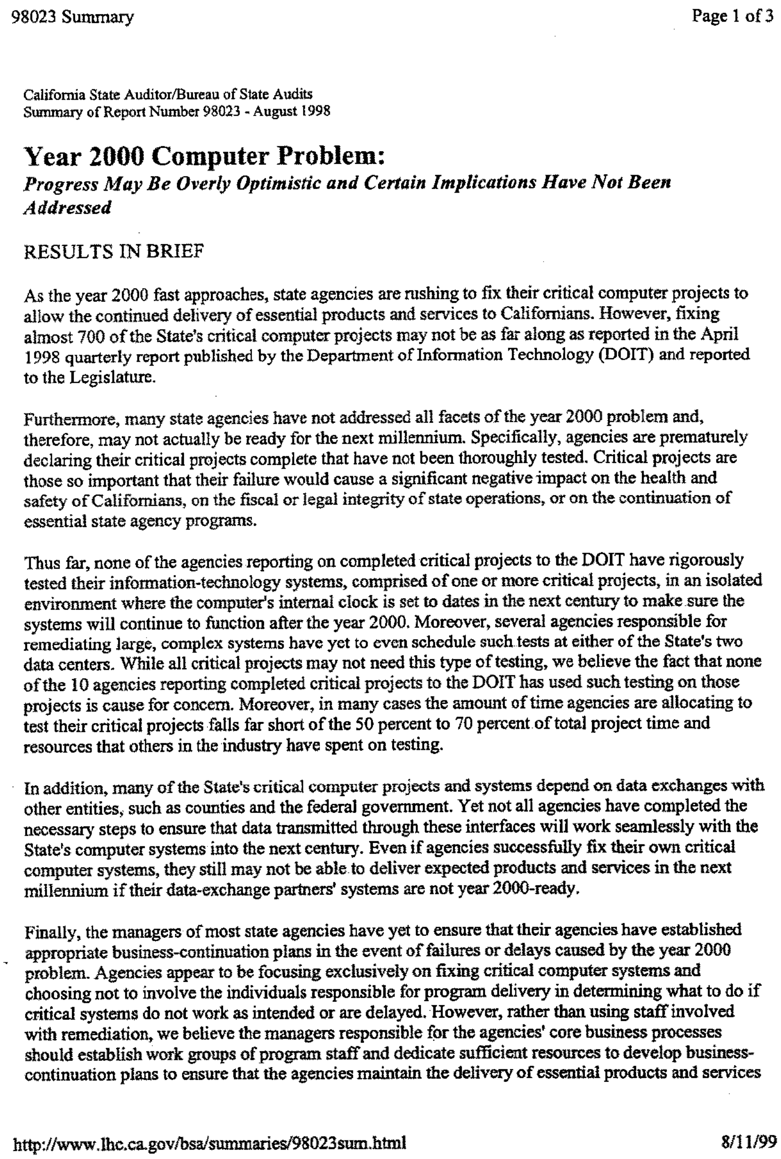


investigate whether they could be at risk of system interruptions, Teale should notify the six clients that used an earlier software version in its time machine environment. Finally, to avoid the potential for data corruption and instability in its operating system, Teale should remove any noncompliant software products from its computers before January 1, 2000.

AGENCY COMMENTS

The governor's office (office) agreed with our findings and stated that the new administration is keenly aware of the challenges posed by the year 2000 problem. The office also stated that the governor will soon announce a plan that will address the issues identified in our report. The Teale Data Center (Teale) agreed with our recommendation that it notify clients that used an earlier software version in its time machine. Teale disagreed with our conclusion that it lacked a successful strategy for its year 2000 remediation plan, but is researching methods available to monitor clients' use of its time machine. The Health and Welfare Data Center agreed with our findings but chose not to respond formally.

Download this entire report in Adobe Portable Document Format (PDF)
Return to the home page of the California State Auditor/Bureau of State Audits



California State Auditor/Bureau of State Audits
Summary of Report Number 98023 - August 1998

Year 2000 Computer Problem:

Progress May Be Overly Optimistic and Certain Implications Have Not Been Addressed

RESULTS IN BRIEF

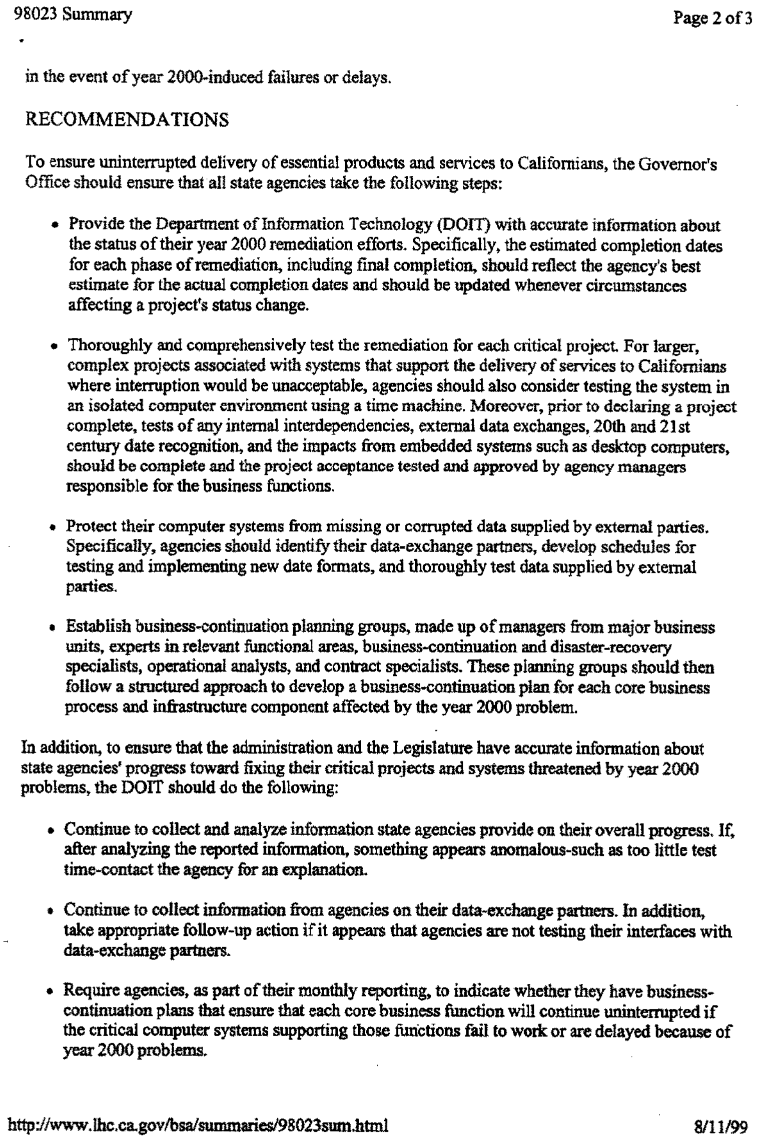
As the year 2000 fast approaches, state agencies are rushing to fix their critical computer projects to allow the continued delivery of essential products and services to Californians. However, fixing almost 700 of the State's critical computer projects may not be as far along as reported in the April 1998 quarterly report published by the Department of Information Technology (DOIT) and reported to the Legislature.

Furthermore, many state agencies have not addressed all facets of the year 2000 problem and, therefore, may not actually be ready for the next millennium. Specifically, agencies are prematurely declaring their critical projects complete that have not been thoroughly tested. Critical projects are those so important that their failure would cause a significant negative impact on the health and safety of Californians, on the fiscal or legal integrity of state operations, or on the continuation of essential state agency programs.

Thus far, none of the agencies reporting on completed critical projects to the DOIT have rigorously tested their information-technology systems, comprised of one or more critical projects, in an isolated environment where the computer's internal clock is set to dates in the next century to make sure the systems will continue to function after the year 2000. Moreover, several agencies responsible for remediating large, complex systems have yet to even schedule such tests at either of the State's two data centers. While all critical projects may not need this type of testing, we believe the fact that none of the 10 agencies reporting completed critical projects to the DOIT has used such testing on those projects is cause for concern. Moreover, in many cases the amount of time agencies are allocating to test their critical projects falls far short of the 50 percent to 70 percent of total project time and resources that others in the industry have spent on testing.

In addition, many of the State's critical computer projects and systems depend on data exchanges with other entities, such as counties and the federal government. Yet not all agencies have completed the necessary steps to ensure that data transmitted through these interfaces will work seamlessly with the State's computer systems into the next century. Even if agencies successfully fix their own critical computer systems, they still may not be able to deliver expected products and services in the next millennium if their data-exchange partners' systems are not year 2000-ready.

Finally, the managers of most state agencies have yet to ensure that their agencies have established appropriate business-continuation plans in the event of failures or delays caused by the year 2000 problem. Agencies appear to be focusing exclusively on fixing critical computer systems and choosing not to involve the individuals responsible for program delivery in determining what to do if critical systems do not work as intended or are delayed. However, rather than using staff involved with remediation, we believe the managers responsible for the agencies' core business processes should establish work groups of program staff and dedicate sufficient resources to develop business-continuation plans to ensure that the agencies maintain the delivery of essential products and services



in the event of year 2000-induced failures or delays.

RECOMMENDATIONS

To ensure uninterrupted delivery of essential products and services to Californians, the Governor's Office should ensure that all state agencies take the following steps:

- Provide the Department of Information Technology (DOIT) with accurate information about the status of their year 2000 remediation efforts. Specifically, the estimated completion dates for each phase of remediation, including final completion, should reflect the agency's best estimate for the actual completion dates and should be updated whenever circumstances affecting a project's status change.

- Thoroughly and comprehensively test the remediation for each critical project. For larger, complex projects associated with systems that support the delivery of services to Californians where interruption would be unacceptable, agencies should also consider testing the system in an isolated computer environment using a time machine. Moreover, prior to declaring a project complete, tests of any internal interdependencies, external data exchanges, 20th and 21st century date recognition, and the impacts from embedded systems such as desktop computers, should be complete and the project acceptance tested and approved by agency managers responsible for the business functions.

- Protect their computer systems from missing or corrupted data supplied by external parties. Specifically, agencies should identify their data-exchange partners, develop schedules for testing and implementing new date formats, and thoroughly test data supplied by external parties.

- Establish business-continuation planning groups, made up of managers from major business units, experts in relevant functional areas, business-continuation and disaster-recovery specialists, operational analysts, and contract specialists. These planning groups should then follow a structured approach to develop a business-continuation plan for each core business process and infrastructure component affected by the year 2000 problem.

In addition, to ensure that the administration and the Legislature have accurate information about state agencies' progress toward fixing their critical projects and systems threatened by year 2000 problems, the DOIT should do the following:

- Continue to collect and analyze information state agencies provide on their overall progress. If, after analyzing the reported information, something appears anomalous-such as too little test time-contact the agency for an explanation.

- Continue to collect information from agencies on their data-exchange partners. In addition, take appropriate follow-up action if it appears that agencies are not testing their interfaces with data-exchange partners.

- Require agencies, as part of their monthly reporting, to indicate whether they have business-continuation plans that ensure that each core business function will continue uninterrupted if the critical computer systems supporting those functions fail to work or are delayed because of year 2000 problems.

Mr. OSE. I stand corrected. We would like you to give your testimony up here at the podium.

This is Joan Smith, supervisor from Siskiyou County. Thank you for joining us.

Ms. SMITH. Thank you, Congressman Ose. Good morning. I want to thank you for the opportunity to provide testimony for the subcommittee with regards to the year 2000 readiness of local governments. I'm here today speaking on behalf of the Regional Council of Rural Counties [RCRC], which is an organization that represents 27 of California's rural counties. I would like to begin by thanking our distinguished congressional representatives for taking time from their busy schedules to be here in Sacramento today. A warm northern California welcome to all of you.

The issues that we are addressing are of great importance to the communities represented by Congressman Ose and throughout rural California. There are only 140 days left before the year 2000, and we still have much work to do. The Y2K preparedness level of local government varies widely within the State of California. California has 58 counties, 471 cities, and over 2,300 independent special districts. Some are ready right now, but many, most, are not.

Today's hearing is especially important because it concerns the readiness of public services their citizens come in contact with every day. Here's where the rubber hits the road for fire, police and the programs and services counties provide for children and families and the basic services that allow communities to function and the economy to grow. It is vital that the citizens in rural California have confidence that county services will still function and that there are realistic contingency plans should any systems fail.

Recently, the General Accounting Office was asked to identify the Y2K status of key services provided by the Nation's 21 largest cities, as was testified here today.

As of early July, America's largest cities report on average that they have completed 43 percent of the work that will be required for an uneventful transition to the year 2000. Information from the National Association of Counties estimate that only 27 percent of the more than 3,000 counties it represents nationwide have completed Y2K testing. Apparently, more than 2,000 counties have a lot of work to do in the next 140 days.

Siskiyou County Y2K experiences. As was previously stated, I'm from the very top of the State, Siskiyou County. We border—we have a population of approximately 45,000 people, and we're located on the Oregon border, and we lie between the counties of Modoc and Del Norte. Siskiyou County began its year 2000 preparedness program in October 1998, with the formation of an interdepartmental task force.

Mr. Chairman, I just wanted to let you know our Superintendent of Schools, Barbara Dillan does sit on our Y2K task force and they are working with us and bringing things up to date. This task force works to identify essential services for each county department, institute contingency planning, coordinate systems testing, test all essential communication systems by the manufacturer, ensure medical facilities have replaced essential equipment and have additional supplies available, create a coordinated response procedure for potential increase in medical response, including home health patients, address potential increase in law enforcement calls, conduct over 100 community awareness programs, develop planning information for all county departments, cities and special districts in our area.

The county of Siskiyou has worked with our region's electric and telephone service providers to ensure that their systems will be fully functional. We are fortunate that our electric provider, Pacificorp, has completed its Y2K compliance testing. In fact, they have rolled their date forward. They are now in the year 2000. They managed to work out any bugs that they had, and we are still functioning in the year 2000 in our area. The Federal Department of Energy has advised us to prepare for the potential of a 2- to 3-day power outage during the first month of the year 2000.

Siskiyou County has actively worked with other governmental entities in the community in the development and implementation of our Y2K preparedness plan to make the transition to the new year as smooth as possible. We believe that our hard work and advance planning related to the Y2K issue will leave us in good shape for anything that may come our way.

The Regional Council of Rural Counties, in response to this hearing, commenced a survey to gauge the year 2000 readiness of our member counties of which you have a copy of the results before you. While this survey is only a snapshot of rural county preparedness, it does provide an interesting accounting of how local governments perceive they are doing. For your information, we have attached a copy of the survey and a computation.

The first section of the Y2K Compliance Survey asked the rural counties to identify the systems they have checked and if and where any problems have occurred and identified. The responses indicated that they are actively checking programs such as 911 emergency systems, jail functions, data bases, billing/payroll, mobile data systems, communication infrastructure, wastewater treatment and a number of other systems.

Several counties have checked and have made needed adjustments to 100 percent of their critical systems. Many of the counties responded they are not checking systems within their counties, that they are the responsibility of State, Federal or private entities. These systems would include rail crossings, mass transit systems and traffic control systems. However, most of the respondents are working with their telephone, electricity, and water suppliers to ensure that these operations are being examined.

The county of Alpine responded that there are no public elevators in the entire county to check and that their 911 emergency services are provided by Douglas County, NV.

The second area of the Y2K Compliance Survey asked the rural counties to note who they are currently working with to determine their ability to interface with other systems. They indicated they were working with State entities, cities, counties and special districts, schools and community organizations to test specific critical interfaces. The counties of Yuba and Shasta have expressed that they have worked closely with their health care providers. Only five of the counties say they have communicated directly with Federal entities regarding Y2K issues. There appears to be little district Federal-to-county technology interface, with most payment and communication systems being linked between the Federal and the State.

The third section of the survey focused on risk assessment. Most of the counties have developed a formal year 2000 preparedness plan and have completed between 50 and 95 percent of the necessary compliance checks. The 15 counties in the survey assessed their combined current readiness is 73 percent. The counties of Lassen and Alpine indicated they do not have official year 2000 preparedness plans. Most of the counties stated that they are attempting to address the Y2K issues internally, and only two counties, Glen and El Dorado, have hired outside consultants to assist them with their effort.

The responses show that 69 percent of counties currently employ a full-time information technology staff person.

The last section asks the counties to indicate the amount and type of public outreach on year 2000 issues that they have conducted. The survey shows the counties have effectively utilized community forums, media presentations to businesses—media—excuse me—presentations to business and social organizations, and public service announcements to communicate how they are preparing, especially to the elderly community.

Many of the counties have developed a brochure or have posted information on their webpages to inform their community about Y2K issues. Merced County's website is located at 222.co.shasta.ca.us and Shasta County is www.co.shasta.ca.us. They are two very good examples.

Before you is a copy of the Y2K Cookbook. This was developed by Merced County with the assistance of the State of California, the Department of Information Technology or DOIT, as we call it.

In conclusion, for the past 3 years California's rural counties have invested hundreds of hours of staff time, replaced and upgraded hardware and software and have spent millions of dollars to prepare for Y2K. The survey and recent conversations with rural county Y2K representatives appear to indicate that most of the counties will be well prepared for any potential disruptions that may occur due to the changeover at the end of the year.

As stated by several counties, the potential of losing services such as electricity or telephone service is not much greater than the possibility of a severe snowstorm, flood or forest fires, all of which we have survived. We strongly believe that no matter what, everyone should always be prepared in case of an emergency. That means having warm blankets, extra food and water, flashlights and backups for all systems containing program logic.

There has been a fair amount of media attention focused on people acquiring survivalist property in rural areas, food and gas hoarding, and the impact of increased traffic on rural roads as people escape urban areas. These doom-and-gloom forecasts will potentially lead to additional impacts upon county services that will be difficult to assess.

California's rural counties are looking forward to a smooth transition to the year 2000 and are working hard to ensure that our citizens and businesses will not be adversely impacted by the failure of any governmental-operated systems. Thank you.

Mr. OSE. Thank you for joining us, Supervisor Smith.

[The prepared statement of Ms. Smith follows:]

United States House of Representatives
Subcommittee on Government Management, Information and Technology
The Honorable Stephen Horn, Chairman

Year 2000 Readiness

Written Testimony of Joan Smith
Siskiyou County Supervisor
Representing the Regional Council of Rural Counties
August 13, 1999
Sacramento, California

MR. CHAIRMAN AND MEMBERS OF THE SUBCOMMITEE:

I want to thank you for the opportunity to provide testimony to the Subcommittee with regards to the Year 2000 readiness of local governments. I am here today speaking on behalf of the Regional Council of Rural Counties (RCRC), an organization that represents twenty-seven of California's rural counties.

I would like to begin by thanking our distinguished congressional representatives for taking time from their busy schedules to be here in Sacramento today - a warm Northern California welcome to all of you. The issues that we are addressing are of great importance to the communities represented by Congressman Ose and throughout rural California.

There are only 140 days left before the Year 2000, and we still have much work to do. The Y2K preparedness level of local government varies widely within the State of California. California has 58 counties, 471 cities and over 2300 independent special districts. Some are ready right now, but many--most--are not.

Today's hearing is especially important because it concerns the readiness of public services that citizens come into contact with everyday. Here is where the rubber hits the road for fire and police, for the programs and services counties provide for children and families and the basic services that allow communities to function and the economy to grow. It is vital that citizens in rural California have confidence that county services will still function and that there are realistic contingency plans should any systems fail.

Recently, the General Accounting Office was asked to identify the Y2K status of key services provided by the nation's 21 largest cities. As of early July, America's largest cities report on average that they have completed 43% of the work that will be required for an uneventful transition to the year 2000. Information from the National Association of Counties estimate that only 27 percent of the more than 3,000 counties it represents nationwide have completed Y2K testing. Apparently, more than 2,000 counties have a lot of work to do in the next 140 days.

Regional Council of Rural Counties
Year 2000 Readiness

Siskiyou County Y2K Experiences

Siskiyou County, with a population of 45,000, is located on the Oregon border and lies between the counties of Modoc and Del Norte. Siskiyou County began its Year 2000 preparedness program in October 1998, with the formation of a inter-departmental task force.

This task force worked to:

- ✓ identify essential services for each county department
- ✓ institute contingency planning
- ✓ coordinate systems testing
- ✓ test all essential communication systems (by manufacturer)
- ✓ medical facilities have replaced essential equipment and have additional supplies available
- ✓ create a coordinated response procedure for potential increase in medical responses (including home health patients)
- ✓ address potential increase in law enforcement calls
- ✓ conduct over 100 community awareness programs
- ✓ develop planning information for all county departments, cities and special districts

The County of Siskiyou has worked with the region's electric and telephone service providers to ensure that their systems will be fully functional. We are fortunate that our electric supplier, Pacificorp, has completed its Y2K compliance testing. The Federal Department of Energy has advised us to prepare for the potential of 2 to 3 day power outages during the first month of the year 2000.

Siskiyou County has actively worked with other governmental entities and the community in the development and implementation of our Y2K preparedness plan to make the transition to the new year as smooth as possible. We believe that our hard work and advance planning related to the Y2K issue will leave us in good shape for anything that may come our way.

Regional Council of Rural Counties
Y2K Compliance Survey

The Regional Council of Rural Counties, in response to this hearing, commenced a survey to gauge the Year-2000 readiness of our member counties. While this survey is only a snapshot of rural county preparedness, it does provide an interesting accounting of how the local governments perceive they are doing. For your information, we have attached a copy of the survey and a computation of the results.

Inventory/System Status

The first section of the Y2K Compliance Survey asked the rural counties to identify what systems they have checked and if there where any problems identified. The responses indicated that they are actively checking programs such as 911 emergency systems, jail functions, databases, billing/payroll, mobile data systems, communication infrastructure, waste water treatment and a number of other systems.

Many of the counties responded that they are not checking systems that are the responsibility of state or federal entities. These systems would include rail crossings, mass transit systems and traffic control systems. However, most of the respondents are working with their telephone, electricity and water suppliers. The County of Alpine responded that there are no public elevators in the county to check and that their 911 emergency services are provided by Douglas County, Nevada.

Interfaces

The second area of the Y2K Compliance Survey asked the rural counties to note who they are currently working with to determine their ability to interface with other systems. They indicated they were working with State representatives, cities, counties and special districts, schools and community organizations to test specific critical interfaces. The Counties of Yuba and Shasta expressed that they have worked closely with their health care providers. Only three of the counties stated that they had communicated with federal entities regarding Y2K issues. There appears to be little direct federal to county technological interface, with most payment and communication systems being linked between the federal and the state.

Risk Assessment

The third section of the survey focused on risk assessment. Most of the counties have a Year 2000 Preparedness Plan in place and believe that 75-95% of it has been completed. The counties of Lassen and Alpine indicated that they do not have a official Year 2000 Preparedness Plan. All of the counties stated that are they attempting to address Y2K issues internally and have not hired outside consultants, and most have at least one full time information technology staff member.

Public Awareness

The last section asked the counties to indicate the amount and type of public outreach on Year 2000 issues that they have conducted. The counties have effectively utilized community forums, media, presentations to business and social organizations, and public service announcements to communicate how they are preparing.

Many of the counties have developed a brochure or have posted information on their web pages to inform their community about Y2K issues. Merced County's web site located at www.co.merced.ca.us and Shasta County at www.co.shasta.ca.us are two very good examples of rural outreach.

Conclusion

For the past three years, California's rural counties have invested hundreds of hours of staff time, replaced and upgraded hardware and software and have spent millions of dollars to prepare for Y2K. The survey and recent conversations with rural county Y2K representatives appears to indicate that most of the counties will be well prepared for any potential disruptions that might occur due to the changeover at the end of the year.

As stated by several counties, the potential of losing services such as electricity or telephone service is not much greater then the possibility of a severe snowstorm, flood or forest fires - all of which we have survived. We strongly believe that no matter what, you should always be prepared in case of an emergency - that means having warm blankets, extra food and water, flashlights ***and a back-up for all systems that contain program logic.***

There has been a fair amount of media attention focused on people acquiring "survivalist" property in rural areas, food and gas hoarding and the impact of increased traffic on rural roads as people escape urban areas. These doom and gloom forecasts will potentially lead to additional impacts upon county services that will be difficult to assess.

California's rural counties are looking forward to a smooth transition to the Year 2000 and are working hard to ensure that our citizens and businesses will not be adversely impacted by the failure of any governmental operated systems.

If additional information is required regarding this testimony or about the Regional Council of Rural Counties, please contact David French at (916) 447-4806 or by email at davidf@rcrcnet.org.

Mr. OSE. Our last witness is Cathy Capriola from the city of Citrus Heights.

Ms. CAPRIOLA. Good morning. On behalf of the Citrus Heights City Council and our community, I'd like to say thank you for the opportunity to participate in this congressional hearing.

Citrus Heights is in a very fortunate position relative to the year 2000. As Congressman Ose knows, since he served on the Citrus Heights Incorporation Project and was president of that at one time, we are a newly incorporated city. We became a city on January 1st and opened our doors for business to the community in July 1997. So because of that and because of the kind of character of our community and the service delivery, we're in a far better position probably than most of our peer agencies.

There are three reasons that we're somewhat of an anomaly with the year 2000. One is because we are a startup, so we have no legacy systems. All of our technology is new, and we have no custom applications that have been developed in-house through the years. We're just installing our local area network and are completing that and at this point have held off on purchasing any other specialized software until the year 2000 passes.

We also have a limited scope of operations. Because we're not a full service city, again, as a newly incorporated city of 88,000, a number of special districts provide services to our residents. So those individuals in the area of parks and recreation and water retain the programmatic policy and the year 2000 responsibility.

The third area that makes us a little different is we're a contract city, more like some of the southern California cities where we contract back to other jurisdictions and the private sector for services. Specifically back to Sacramento County that provides our law enforcement—very, very well, solid waste, and street and related infrastructure maintenance. So we're coordinating with Sacramento County and private firms that provide services for us and communicating with them.

In terms of what the city has done—a complete inventory and prioritization of what we do have, and that's 98 percent complete. The systems we currently use require some remediation—and even with new technology there are still patches and tinkering that needs to occur. So, we will be completing that within the next 45 days. We're doing some community outreach. We'll be holding some workshops with our community in September and also working with our contracting agency, Sacramento County, et cetera, on emergency operations and some of our mission critical items.

So overall, just to summarize, I think that for we as a city, timing is everything, and we became a city at the right time on this one. And we're in a very fortunate position. Just the way we're structured, being new, we're less complex in scope and smaller than all of our peers. I'd be happy to answer any questions.

Mr. OSE. Thank you, Cathy.

[The prepared statement of Ms. Capriola follows:]

CITY OF CITRUS HEIGHTS

YEAR 2000 COMPLIANCE PROJECT

Presented to:

Congress of the United States, House of Representatives

**Subcommittee on Government Management,
Information and Technology**

**Field Hearing on Year 2000 Readiness of State &
Local Governments, Utilities & Local Industries**

By: Cathy Capriola, Administrative Services Director

Sacramento, California

August 13, 1999

City of Citrus Heights
Year 2000 Compliance Project

PROJECT CONTEXT:

The City of Citrus Heights (population 88,265) is located ten miles east of downtown Sacramento, and is largely a residential community with a strong retail economy. The City incorporated in January 1997, and began providing municipal services in July 1997.

As a municipal corporation, Citrus Heights is in an uniquely fortunate position with relation to Year 2000. There are three reasons for this – new technology, status of not being a full service city, and the contract nature of a majority of our service delivery.

1. New Technology – As a newly incorporated City, we are fortunate to not have any legacy systems – either software or hardware. We are just completing installation of our local area network and have purchased all our desktop systems within the last 2 years. We have also been careful to limit our investment in vertical market software applications at this time. Finally, we are fortunate to have no custom applications that have been developed in-house and required reprogramming.

2. Not a "Full Service" City -- Also, due to such a recent incorporation, the City of Citrus Heights is not a "full service" municipality. Several special districts such as fire protection, parks and recreation, sewer, and water have been providing services to Citrus Heights residents for decades. Therefore, the responsibility of Year 2000 within these functional areas falls upon those agencies.

3. Contract City – Thirdly, Citrus Heights is organized as a "contract city" – a large segment of the City's services are contracted to private firms or other governmental agencies. For example, the City contracts with private firms to provide planning, building, and engineering services. Via contract, Sacramento County provides law enforcement, solid waste, street and related infrastructure maintenance, drainage, and other public works oriented functions. Regional Transit provides public transportation services for the City. In these functional areas, again, the responsibility of Year 2000 is the responsibility of these contracted agencies.

YEAR 2000 PROJECT-AT-A-GLANCE:
The City's approach is to ensure corporate compliance by Fall 1999 and continue to monitor contractors and related special districts for their compliance.

PHASE 1 – INVENTORYING & PRIORITIZATION OF ASSETS (98% complete)

- Inventorying of all computer hardware
- Inventorying of all computer software
- Inventorying of all "in house" developed applications
- Inventorying of all facility systems
- Inventorying of all non-computer hardware (desktop hardware with embedded chips)
- Coordinating with all City contractors and vendors
- Reviewing computer and facility system redundancy
- Sent letters for letters to vendors and service providers to determine Year 2000 compliancy

City of Citrus Heights
Year 2000 Compliance Project

PHASE 2 -- PRIORITIZATION & REMEDIATION (90% complete)

1) City Corporate Assets
   - Local area network (90%; completion date by 8/31/99)
   - Desktop computers (114 systems; hardware 95% completed; software 60% complete -- 9/30/99 target completion)
   - On-Site Contractor Assets – (databases & templates; telecommunications; minor software modifications – 9/30/99 completion)
   - Telecommunications system – compliant
   - Facilities (elevator, HVAC, alarm and electric gate; compliant now)

2) Other Entity Controlled Assets – Contract, Private, or Special Districts
   - Police Department (via Sacramento County); 800 mhz radio system, 911 & non-emergency numbers, patrol cars
     - Compliancy letter received
   - Continuing to monitor and review compliancy status from other organizations providing service to the City and the Citrus Heights community.

PHASE 3 – COMMUNITY NEEDS & PUBLIC OUTREACH (85% complete)

- Joint public meeting with local service providers including (PG&E, SMUD, Telephone, three Water Districts, Cable TV, City of Citrus Heights, Sanitation District & Fire District)—interactive meeting format—to be held in the early fall
- City Council presentations; City newsletter article; press releases
- City presentations in the community on a requested basis

PHASE 4 – EMERGENCY OPERATIONS (In process)

- Staff discussions regarding emergency operations needs and final strategy underway.

For further information, contact Cathy Capriola, Administrative Services Director or Hilary Straus, Management Analyst at 916-725-2448.

Mr. OSE. Now, as far as how we proceed from here, many of you have not participated in a congressional hearing. What we do is the chairman and I will direct questions at the witness and you're free to answer. If there is something you care to add to someone else's testimony, be happy to take that testimony.

So with that, Mr. Chairman, would you like to proceed?

Mr. HORN. Well, let me ask Mr. Willemssen, who has been a faithful attender at every single one of our field hearings for the last 3 years, what you heard this morning, how does that fit in with other things the General Accounting Office has looked at in other areas and States? And are we missing something here that we should ask about, and what do you think it is?

Mr. WILLEMSSEN. One area that you might want to pursue with some of the witnesses, I realize the State IT director is no longer here, but I heard touched on very briefly but you may want to pursue a little more, testing of data exchanges with other organizations.

Many of the witnesses talked about where they are at with their own systems and they are making great progress; but as you know as well as anyone, the testing of data exchanges is especially critical to make sure that there aren't any disturbances that affect the systems outside of your control. And I think your question earlier to the State Director on the education side again points to that.

I know that Secretary of Education has expressed great disappointment with the low number of schools who have opted to test their data exchanges with the Federal Department of Education on loans and grants. And I think that it would be worthwhile for California, among other States, to begin looking at how well their postsecondary schools are actually doing in the testing of those exchanges, because my understanding is nationally it still remains a very low number who have taken advantage of it.

Mr. HORN. I think you're correct. I wrote a letter to the Secretary of Education Riley about a month and a half ago. I don't think we have an answer to it yet, but our feeling was given the lack of money in many school districts and the smaller ones along the Pacific Coast where you've got a lot of rural schools still, and I'm proud to say I went to one, I thought I got a great education, but the fact is this takes money. And I think I told him to make an estimate for us and see what's needed and would they administer the program.

Mr. WILLEMSSEN. The other thing I might add, Mr. Chairman, is taking a look at the California State Auditor's Report of February 1999, I thought that raised some good issues. The question, if I were in your chair that I would want to ask, is what their plans are for upcoming review, if they have an audit or report that is due to be issued so there could be some check on the statements that were made by the State director of IT.

Mr. HORN. What plans does the State Audit operations have?

Mr. CORDINER. The way our office operates, we do audits at the request of Joint Legislative Audit Committee and thus far they have not asked us to do any further work in this area. However, based on our prior reports, we do get periodic updates on the progress of our recommendations and whether they've been implemented or not; and insofar as that goes, a lot of what Mr. Cortez said we're encouraged by, the planning that has gone into this. And the new administration, obviously they've dedicated considerable resources. We're still somewhat concerned, however, in that the last quarterly report that was generated by the Department of Information Technology which came out in July indicated while a number of agencies that are deemed critical agencies that have programs that are highly necessary for Californians and that they depend on have progressed, they're still—one of the things that is measured and you were concerned earlier with was, "Well, how much independent work has been done?"

Now, clearly there has been independent work done on assessing where they are currently at to get a measurement, but another part of DOIT's planning is to have an independent verification and validation of those very critical systems to see, "OK, they are ready for the date change." That has not occurred in any of the ones that are listed on the website, to my knowledge. And so there is still a concern in that area.

In addition, we had recommended in our February 1999 report that particularly for critical programs that business continuation planning be done by June 30, 1999 which mirrors industry standards so that there's enough lead time for those that require hiring additional staff or whatever the work around is going to be for that to occur. In addition, to be able to test that plan to see if it's viable.

And we saw again in the last quarterly report that those plans are being requested. They drafted them in August and the final in September, and now I see in the prepared comments that that date has slipped even further, and so they are looking for one that's been fully tested in October. Well, if they fall short of the mark, that's pretty close to an immoveable date. So we've got some concerns in that area.

I failed to mention in my statement because of the time constraints that one of the issues we looked at in the February 1999 report was also to survey every State agency that was in the Governor's budget. 140 of them are responsible for 460 programs. We found that for two-thirds—nearly two-thirds of the programs or the systems supporting the programs they operate, one or more critical steps wasn't completed at that point in time, which was December 31, 1998, and that nearly one-half of the agencies did not have business continuation plans.

Mr. HORN. You're absolutely right. In terms of verification approach, and I wondered if as the welfare system in the State with the Federal billions and the State billions and then the county welfare in 58 counties, what is the interconnection there between the smaller welfare groups like San Benito and San Luis Obispo?

Mr. CORDINER. As far as the Y2K exposure, a lot of it is the interface that Joel mentioned earlier. It's critical both upstream and down for State agencies to be able to seamlessly communicate with both the Federal, local and outsiders. Say, Medi-Cal, for instance, has third-party providers. It's a tremendous amount of interface that goes on.

Mr. HORN. Has much of that been tested, to your knowledge?

Mr. CORDINER. To my knowledge, the quarterly report—in fact, I looked at the appendix that was attached to that that lists every one of the departments, and some indicated that they completed testing, or at least say they have, or an independent party says they have without the independent verification of it that they have tested their data exchange. For others, that information was not included, when we've known based on our past work that these systems that didn't indicate anything about data interchange do have that. So I don't know what the status is, to tell you the truth.

Mr. HORN. This question isn't necessarily on the year 2000, but it's a computer question, and that's the deadbeat dad situation. In Congress we had to get an exemption for California because you would have had a lot of money taken away since I think—what is it—about 24, 25 counties don't like the L.A. system and wanted their own system, and where are we on that?

Mr. CORDINER. The current status on that—it's fortuitous you ask. I was on that. We just released an audit report on the 5th on that. What California tried to do is create a consortia which would have been a link—four systems, including Los Angeles, would have been linked together, and that would have been the State's plan to develop a statewide automated child enforcement system. That was recently rejected. That plan was rejected at the Federal level.

We are now back to basically square one where the Health and Welfare Data Center which is responsible for developing the IT solution for this program has awarded four different contracts to vendors to come up with a design. The winner of that will be given a future contract to develop or replicate an existing system for California to use. So we're—in my mind, we're years away from a statewide automated system. There are systems in use out there, and the ones that we visited, most of them are Y2K ready now. Some weren't and they were migrating to other systems that were.

Mr. HORN. Thank you.

Mr. OSE. If I may follow up on something, Mr. Cordiner, in your testimony you talked about noncompliant products being used I believe at the Teale Data Center?

Mr. CORDINER. Correct.

Mr. OSE. After the Teale data operator advised everybody not to use those same products, and my question is whether or not we're still using those noncompliant products?

Mr. CORDINER. Based on their last response to our audit, those have been—they are in the process of removing them.

Mr. OSE. That was the critical question, whether they complied with their own recommendation.

Second, if I might, I know that the director of—I like the acronym DOIT—the director of DOIT testified about the independent verification validation, but in your opinion, are those truly independent?

Mr. CORDINER. We haven't really reviewed—I know they had established a prequalified pool of vendors that could meet the need. We didn't really look at that process and we haven't really evaluated what's being done in the IV&V to determine that. The answer to that question, I would hope that they are. And I think you know this isn't about pointing a finger.

Mr. OSE. I understand.

Mr. CORDINER. And I think Mr. Cortez is sincere in wanting this to be done the best possible way. So with that in mind, I'm confident that those people are doing a good job.

Mr. OSE. Do I understand that your charge to do an audit follows a request? In other words, you cannot move independent of having received a request either from the Governor's office or the Legislature?

Mr. CORDINER. That's correct.

Mr. OSE. OK.

Mr. HORN. If I might ask one more question.

Mr. OSE. Certainly.

Mr. HORN. One question comes to mind, having read in The Sacramento Bee this morning makes me ask this, a 15-year-old that knifes and kills a woman older than him, and he's out as a juvenile and should have been locked up earlier. And that gets down to what's happening in a number of States when they checked for 2000 conformity, they found their jail/prison security systems are opening the doors sometimes. And unless they check that, you're going to have a real problem. I wondered in terms of the sheriffs and State and if the audit team has gone into any of that?

Mr. CORDINER. We—in our last audit, we looked at the Department of Corrections and we looked at two specific systems. One was where the prisoners were at. You know, their status, reporting status. We found that to be OK. The other was an imbedded chip issue with the electrified fences that encompass 23 of 33 institutions. They still had work to do on those, so there was no assurance that those work as intended.

It's my understanding that Mr. Cortez had a group of independent contractors go out and see where that was at, but I see on his website that Corrections still is designated with a pink, which is a high-risk element associated with their ability to be ready at the appropriate time. We were assured, however, during hearings that Corrections has backup systems to those electrified fences whereby if push came to shove they would have 24/7 guards in the towers. So hopefully we can sleep a little bit better knowing that.

Mr. HORN. Yeah. Interesting.

Mr. OSE. Supervisor Smith, the question I have is given the nature of my district, seven of my eight counties are effectively rural, what are the unique challenges that the rural counties are facing? Have we been helpful? Has the State been helpful and what can we do to assist solving those problems that are unique?

Ms. SMITH. Well, Congressman, as I had mentioned, we have the Y2K Cookbook which the State did assist in; and going on line, I believe, is very helpful with the smaller counties that don't have the ability to hire the technology. In Siskiyou County we're fortunate that we do have a technology staff, if you will. Small, but they've been helping us with what our Y2K task force has come forward with. I was surprised to see the small amount of interface with the Federal level. So most of our interface comes up at the State level. So we are working with the State.

What our biggest challenge right now is I think we've gone in internally and we've done our planning there, but I believe what our biggest challenge is and what we're in the process of doing is getting out to the public. We're going into the smaller communities.

We're finding that we're getting calls on a daily basis from the elderly community who are very concerned and frightened, "What if the electricity goes out?" It's very, very cold in Siskiyou County in January, and they are concerned about heating and about telephones. So we're getting out to the public. We're telling them what we've done. We're also advising them to have—as I had mentioned in any emergency, to have things on hand in case of an emergency: Warm blankets, extra food, extra water, for at the most a 2- to 3-week period, but we're saying 2 to 3 days as has been advised, I believe, by the State and Federal Government.

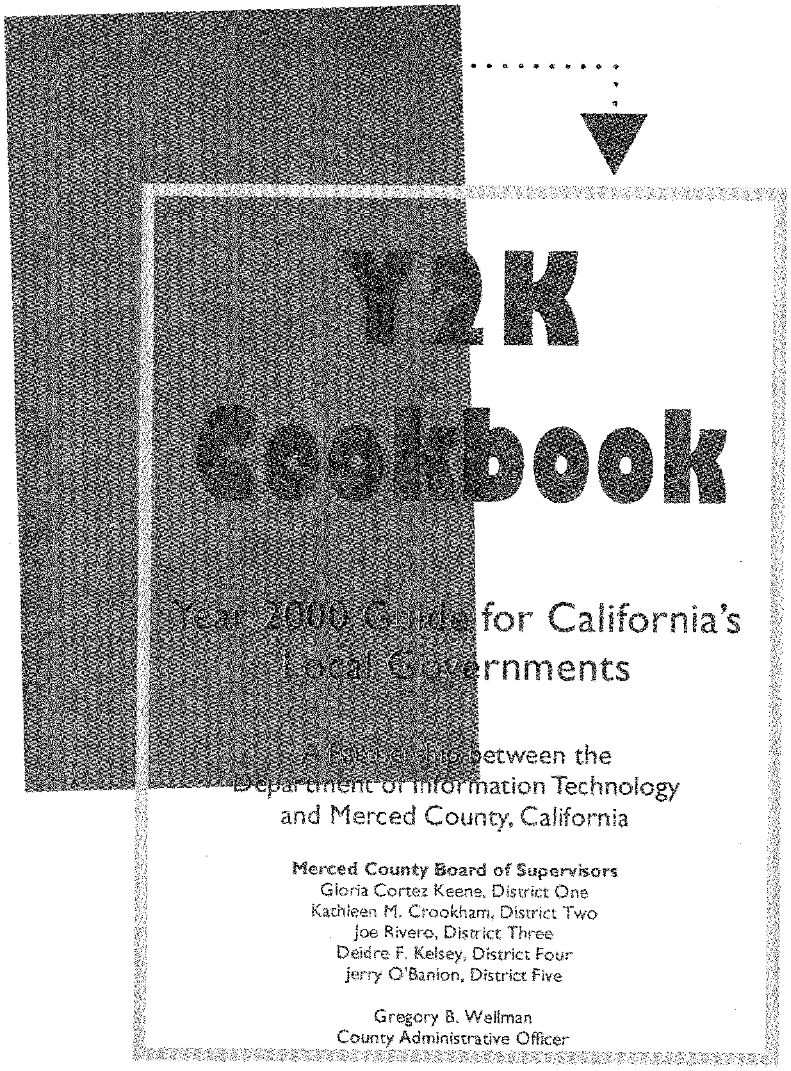
I think that having some funding available which I believe the State has some available, I'm not sure at the Federal level, it's very helpful for some of the smaller counties. As you know, the budgets are very restrictive in the smaller counties and we don't have a lot of extra money, although Siskiyou County has been in the process of replacing a lot of our computer system and we have spent probably half a million dollars doing that and we will probably be spending another $100,000 between now and the end of year in replacing the things that we have to. We are also are hoping we will be up and ready to go by at least October because, as Mr. Cordiner said, in October there is not a whole lot extra you can do at that time.

Most of the counties—I was surprised and pleased to see that most of the counties are addressing this issue. I think that in the area—many of the areas that has not been addressed are the very small areas such as the service districts and small water companies and we're working very hard to work with them. It would be nice if the State would help us with that and the Federal Government, Because they just don't have the staff to do it nor the money, and those are the areas that we're concerned about.

Mr. HORN. If I might, Mr. Chairman, without objection, I'd like to see the Merced document entered into the record in full.

Mr. OSE. Without objection.

[The information referred to follows:]



Y2K Cookbook

Year 2000 Guide for California's Local Governments

A Partnership between the Department of Information Technology and Merced County, California

Merced County Board of Supervisors
Gloria Cortez Keene, District One
Kathleen M. Crookham, District Two
Joe Rivero, District Three
Deidre F. Kelsey, District Four
Jerry O'Banion, District Five

Gregory B. Wellman
County Administrative Officer

Merced County
2222 M Street
Merced, CA 95340
209-385-7434
www.co.merced.ca.us

TABLE OF CONTENTS

Y2K Cookbook

INTRODUCTION

This ***Y2K Cookbook*** is the result of a partnership project between the State of California Department of Information Technology and Merced County, California. Under direction of Governor Gray Davis, a State Year 2000 and Information Technology transition team examined multiple layers of Y2K issues. One conclusion identified was the need for the State of California and its local counties to cooperate together to minimize Y2K-related disruptions. The team proposed a pilot project where the State would collaborate with a county to review and evaluate the county's Y2K remediation efforts. To this end, the Department of Information Technology and Merced County joined together to develop a prototype assessment program, which could be used by other local governments to enhance preparedness for the Year 2000.

This project was a valuable opportunity for the purpose of helping to ensure that California – its citizens and businesses – are afforded the smoothest possible transition to the Year 2000, and that they are not adversely impacted by any failure on the part of California's governments to effectively deal with the Year 2000 problem.

It is our hope that local governments facing the Y2K challenge will be well equipped and prepared to usher in the new millennium.

Merced County Board of Supervisors
Gloria Cortez Keene, District 1
Kathleen M. Crookham, District 2
Joe Rivero, District 3
Deidre F. Kelsey, District 4
Jerry O'Banion, District 5

Gregory B. Wellman
County Administrative Officer

OVERVIEW

Year 2000 is fast approaching and it is imperative that California's state and local governments are prepared to continue critical business functions with few, if any, disruptions due to the changeover at the end of the year. With the increased dependence on technology, state governmental entities regularly work in concert with local government organizations to deliver services to the public. The result of this interdependency is that if the computer system of one governmental entity is disrupted, it could affect the automated operations of other governmental entities. Therefore, it is essential that local government be successful in Year 2000 remediation efforts because of the vital role local government plays in the delivery of essential services to the state's 33 million citizens.

This ***Y2K Cookbook*** shares the lessons learned from the partnership project between the State of California and Merced County. It will outline the same steps taken to complete a preparedness evaluation for Merced County. Other local governments must realize that this Guide is not an all-inclusive handbook; rather it is a tool intended to share with others what was learned and gleaned from the experience. Merced County claims no expressed or implied warranty for the methods contained herein. Therefore, use this as a Guide for Y2K efforts, acknowledging that each entity is unique to itself, with its own challenges and vulnerabilities.

INVENTORY

LIST EVERYTHING

The first thing that any organization should do is to create a list of automated systems that might be affected by the Year 2000 problem. Enlist the help of everyone in the organization to identify all systems that contain program logic.

The following is a sampling of items to consider:

> ⌘ ***Think broad! Y2K is more than just a computer-related problem. It can affect any automated system.***

- Public Works Hardware
- Flow Control Devices
- Global Positioning Systems
- Elevators
- Power Plants
- Security Systems (Doors, Locks, etc.)
- Water Treatment, Potable
- Waste Water Treatment
- Plumbing Systems

- Transportation Systems
- Freeway Metering Systems
- Highway Transportation Controls
- Mass Transit Systems
- Rail Automated Switching Systems
- Traffic Light Controllers

- Communications Infrastructure
- Microwave Communications Systems
- Telephone Switches (Pagers, Cell Phones, Telephones, Phone Cards)

LIST EVERYTHING - Continued

- Management/Maintenance Systems
- Other Mainframe Applications
- Payroll Systems
- Billing Systems
- Permit Applications Systems
- Police CAD Systems
- Procurement Applications
- Wanted Vehicle Systems
- Revenue Systems
- Street/Location Systems
- Loan/Mortgage Systems
- Public Records Indexing Systems
- Utility Billing Applications
- Wanted Persons Systems
- Hand-held Software (Parking Tickets, Meter Reading, etc.)

- Data
- Mainframe Databases
- Network Server Databases
- Personal Computer Databases
- Computers
- Desktop Computers
- Mainframes
- Software on Mainframes
- Network Computers
- Mobile Data Terminals
- Hand-held Computing Devices
- Software on Networks or Desktops
- Electronic Spreadsheets

- (Ad Valorum) Tax Systems
- Criminal Records Systems
- Criminal Justice Systems
- Drivers Licensing Networks
- Financial Management Systems
- Finger Print Identification Systems
- Fire CAD Systems
- Human Resource Systems
- Identification Systems
- Inventory Control Systems

- Alarm Systems (Clocks)
- Cash Registers
- Pocket Organizers
- Travel Services
- Office Equipment (Photocopiers, Fax Machines, Post Scales, Video Equipment)
- Banking Hardware (ATM Machines, Credit Cards)
- Banking Services (Funds Transfer, Clearing Services)
- Citizen Services (Library Cards)

- Hospital Equipment
- Health Records Databases
- Air Traffic Controls
- Vehicle Automated Systems

INVENTORY

GATHER INFORMATION

When all potentially affected systems have been identified, collect information on each system. The information will assist in prioritizing the most critical systems for an organization. Most organizations will not finish remediation on all of their systems. Therefore, every organization must carefully prioritize its applications, putting what is most critical to its self-preservation first. Collecting basic information from the users, developers and vendors of each system will ensure that the task of prioritization is an educated decision.

It is essential that the information collected is complete, clear and accurate. The depth and breadth of time spent on gathering data can be as long or as short as needed. The quicker course includes obtaining very basic data such as the following:

- Name and Description
- Location
- Date Dependency
- Embedded Processor Included
- Number of Users
- Contact Person

A more detailed profile of the system would add:

- Developer/Vendor
- Primary Functions
- System Interfaces
- Volume and Rate of Transactions
- Software Platform, Operating Systems, Language, Size
- Analysis Method
- Remediation Methods and Status

Refer to Form A – Department Inventory and Form B – Critical System Evaluation in the Appendix for examples of forms used to gather information.

SOFTWARE SYSTEMS

There are basically two types of software: commercial-off-the-shelf software and custom developed software.

For commercial-off-the-shelf software, an organization will obtain information from the software manufacturer. Most companies have Internet websites publishing whether their applications are Y2K compliant. An organization will want to obtain a letter or certificate of Y2K compliance or specific plans for becoming compliant. Additional measures that add depth to the evaluation include the fixing logic, test methods and reports. If a software program will not be compliant, be sure to obtain from the manufacturer suggested workarounds.

Refer to Form C – Y2K Certification Request in the Appendix for sample letter of request.

Custom developed software refers to the "home-grown" application programmed for specific purposes or departments within an organization. Many local governments have information technology departments, which write mainframe applications. Evaluation of custom software systems will enable the organization to determine how much of the system is complete and Y2K compliant.

EMBEDDED SYSTEMS

Local governments will be surprised to know that there are more embedded systems at large in the organization than estimated. Essential business components depend on the operation of microelectronic circuits known as "embedded systems".

Like commercial software manufacturers, most companies have Internet websites publishing whether their equipment (wherein the embedded system may be located) is Y2K compliant. An organization will want to obtain a letter or certificate of Y2K compliance or specific plans for becoming compliant. Additional measures that add depth to the evaluation include the fixing logic, test methods and reports. If a specific embedded system will not be compliant, be sure to obtain from the manufacturer contingency suggestions.

There are also specialty firms, which address embedded system issues. These firms inventory all known embedded systems in buildings and vehicles. They evaluate and provide an assessment as well as recommendations of actions for remediation.

INTERFACES

It is hard to imagine any organization as a separate entity. In today's world, many local governments are realizing that interdependencies are rampant. Many local governments may use state or federal systems, or be linked with school systems, or partner with business services. These interface relationships must be included in the evaluation of an organization's systems. Although each entity may pursue separate Y2K efforts, collaboration is essential for successful Y2K compliance.

⌘ ***Who do you interface with?***

Evaluating interfaces demands that organizations network, communicate and share information. Identify external relationships and interfaces when gathering data. Interfaces may include:

- Federal Government
- State Government
- Counties
- Cities and Municipalities
- Special Districts and Agencies
- Businesses
- Community Organizations
- Schools
- Citizens

RISK ASSESSMENT

Once the inventory is complete, the organization should assess the risk involved with each system. The assessment includes measuring the progress of the remediation activities for different types of systems.

YEAR 2000 PREPAREDNESS

Each organization needs to determine critical deadlines or completion dates to measure the readiness of the various systems. When identifying key dates, ensure that adequate time is allotted for testing. It isn't enough to merely finish programming before December 31, 1999. It is equally important to have thorough tests concluded well before the rollover.

⌘ ***Will the system be ready by your critical dates?***

BUSINESS CONTINUITY PLANS

It is recommended that an organization take all necessary steps to ensure the continuous delivery of essential services. Include in the organization's assessment a review of contingency plans. Contingency planning involves designing "What if?" scenarios with multi-layered alternatives, including manual processes. For each system, especially those identified as most critical, the organization should have pre-planned response activities to react to failure scenarios. Depending on the criticality of the system, it may be necessary to have more than one backup plan in place.

There are various methods for providing business continuity. An organization will discover that some systems, such as a power generator, are backups for others. Having a manual process or procedure or other systems or individuals who perform the same process are other options, while some systems may not have a continuity strategy.

UNAVAILABILITY IMPACT

When conducting a risk assessment, ensure that impacts caused by unavailability of systems due to Year 2000 problems are identified and assessed. While few applications would actually impact public safety or property loss, many could cause varying levels of hardship on employees or clients. The organization must always consider the consequences of not being able to use a specific item.

⌘ ***What would happen if the system were not available for use?***

Losing the function for receiving 911 emergency calls or dispatching emergency vehicles (either police or fire) could create a critical situation where public safety is in jeopardy or public property is at risk. Or the loss of power could make most traffic signals and railroad crossing controls inoperative, potentially causing personal injury or property loss.

Other systems, which could cause varying degrees of hardship, revolve around the organization's ability to meet its day-to-day obligations. These include:

- Wide or Local Area Networks (Personal Computers and Application Software)
- Mainframe Computer Systems (Peripheral Equipment and Application Software
- Public Assistance Benefit Delivery and Reporting (Cash and Food Stamp)
- Payroll (for General Staff, Retirees and General Service Providers)
- Probation Case Management
- Juvenile Hall Operation
- Financial Management Systems (Accounts Payable, General Ledger, Cost, etc.)
- Telephone Systems
- Public Facilities Management and Control (HVAC, Elevators, Alarms)
- Correctional facilities (Alarms, Automatic Controls, Lighting, Booking and Release Information)
- Mental Health and Public Health Case Management Tools
- Jury System
- Court Calendaring
- Criminal Warrant Processing
- Family Support Collections and Disbursements
- Revenue Collections (Utilities, Taxes, etc.)

DOWN TIME TOLERANCE

Another indicator of the risk involved with a particular system is predicting the down time tolerance. Any organization should ask itself how long could a system be down until it causes a significant impact. For instance, an email system could be down for 10 days with little impact; however, the failure of the correctional facility automated cell locking system will have instant impact. The automated cell locking system cannot tolerate any down time to occur.

⌘ How long can you manage, if the system was not available?

Systems that have a low volume in use can be allowed to be down and inoperable for longer periods of time. Organizations may find that there is no tolerance level for certain systems, such as backup generators systems. The level of tolerance for down time will vary between organizations as well as between departments and even users within the organization.

PRIORITZE

Prioritization is defining the focus of Y2K efforts for an organization. Based on the information gathered in the inventory, key organization staff will determine what systems demand immediate attention. An organization must identify and prioritize functions that must be made Y2K compliant immediately and those other functions, which can be addressed later. Prioritization will focus energies on what will have the most impact.

For a local government, there are many things to consider, and each organization needs to develop its own strategy for determining priorities. Some basic categorical impacts to consider in terms of prioritization include:

⌘ What matters most to your organization?

- Public Safety – threatens the public (alarm/security systems, correctional facility locking systems)
- Life Threatening – poses immediate danger (911 emergency services, life support systems)
- Officer Safety – threatens peace officers (criminal databases)
- Health and Welfare Services – impacts citizens (welfare check printing systems)
- Financial Stability – threatens revenue streams (tax and billing systems)
- Legal Implications – compromises legal requirements (court systems)
- Public Services – decreases services to citizens (library cards, recreational facilities)

Other information to consider comes from the risk assessment of the each system. Systems that have backup sources, contingency plans, manufacturer certification, testing validation are better prepared than others. When completing the task of prioritization, always ask what kinds of impacts would unavailability or non-compliance have on the members of the organization.

Local governments are in a precarious position, as a provider of services to thousands of citizens. The impact of Y2K will not only affect members of the local government organization, but all citizens within as well as outside of its boundaries. Thus prioritization is essential to the Y2K efforts of an organization.

SOLUTIONS

REMEDIATION AND MITIGATION

While an organization may hope to have every possible issue fixed, many will have to settle on a combination of remediation and mitigation efforts.

Remediation is choosing to fix the problem. There are generally five technical solutions to the Year 2000 problem:

- Conversion – change every date to a four-digit year
- Fixed windowing – create a 100-year window such as 1929 and 2029 and if the two digit year is greater than 29, then the program assumes the century digits to be 19; if the two-year digit is less than or equal to 29, the century digits are assumed to be 20
- Sliding windowing – similar to fixed windowing except the 100-year window is calculated from the current date
- Encryption –compress dates with four-digit years to occupy the same storage space as dates with two-digit years
- Encapsulation – reset the year to 28 years earlier, useful only in embedded process controllers in which the year is not important but the day of the week is important

Remediation can be demanding and time consuming, especially for an organization that relies on customized application software. There may be millions of lines of program code to change, as well as invalid date comparisons.

Opting to mitigate a problem means that the organization will create a plan that works around the problem. It could be replacing a system with a newer Y2K compliant version or reverting to a manual process. It may also require simply dealing with a usable but non-compliant non-critical system until a later date when it can be remediated.

Refer to Form D – Sample Mitigation Plans in the Appendix mitigation suggestions.

PUBLIC AWARENESS

SHARE INFORMATION

All organizations, especially local governments, should include in their Y2K efforts public awareness. The more informed people are, the less fearful they behave. There is so much information in the news about the Year 2000 problem ranging from the switch marking the end of the world or the optimistic opinion that Y2K will not cause a single problem. Individuals should realize that the reality will lie somewhere between those two extremes.

Organizations are encouraged to share their work and progress with its internal associates as well as its external customers and constituents. Honest communications will inform the public of what services are guaranteed available, precautionary measures to take and business continuity plans that will be in place. Local elected officials are encouraged to partners with business and community leaders to collaborate. Ideas for raising public awareness include:

- Community forums
- Regular media publications
- Business roundtables
- Outreach programs
- Public service announcements

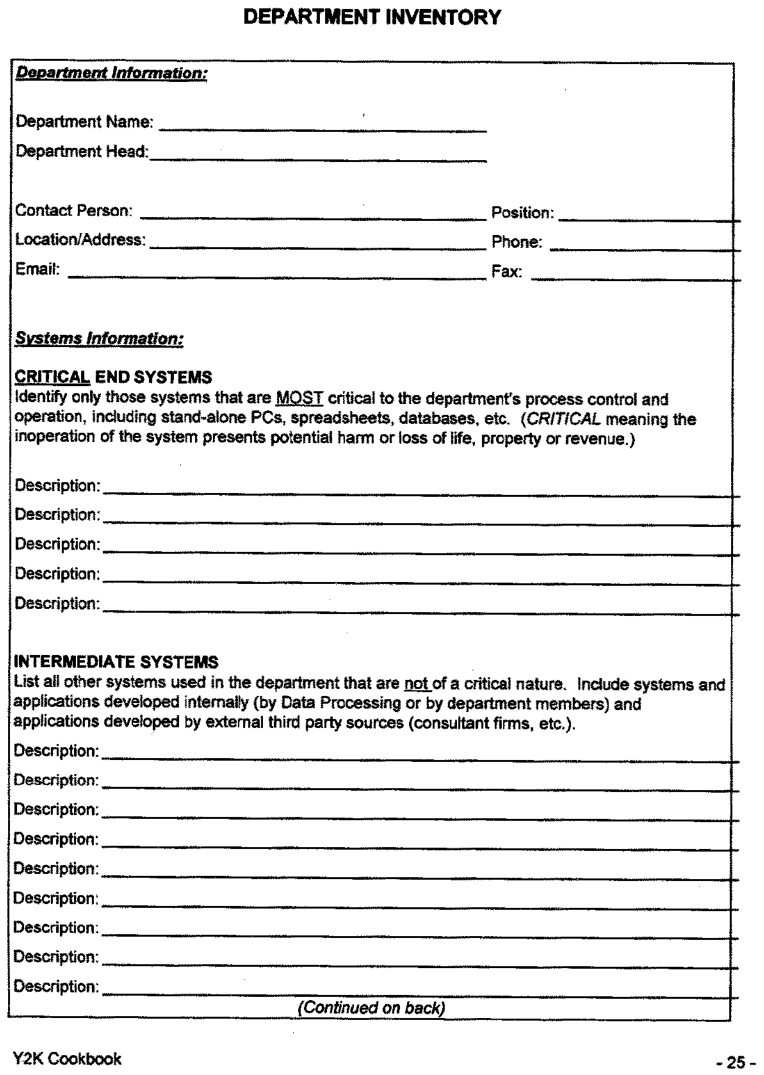
CONCLUSIONS

The Year 2000 is a real problem and organizational preparation is essential to ensure that the citizens of the State of California are not adversely impacted. The majority of potential Year 2000 problems discovered within local governments can be identified and anticipated using the following steps:

- Start today.
- Inventory everything.
- Acknowledge and assess the organization's vulnerabilities.
- Focus on what is most critical to your organization and tend to those items first.
- Have a plan in place to ensure that business continues as best as possible.
- Share your progress and status both internally and externally to increase awareness and reduce fears.

APPENDIX

- Form A Department Inventory
- Form B Critical System Evaluation
- Form C Y2K Certification Request
- Form D Sample Mitigation Plans



DEPARTMENT INVENTORY

Department Information:

Department Name: ____________________

Department Head: ____________________

Contact Person: ____________________ Position: ____________

Location/Address: ____________________ Phone: ____________

Email: ____________________ Fax: ____________

Systems Information:

CRITICAL END SYSTEMS

Identify only those systems that are MOST critical to the department's process control and operation, including stand-alone PCs, spreadsheets, databases, etc. (*CRITICAL* meaning the inoperation of the system presents potential harm or loss of life, property or revenue.)

Description: ______________________________

Description: ______________________________

Description: ______________________________

Description: ______________________________

Description: ______________________________

INTERMEDIATE SYSTEMS

List all other systems used in the department that are not of a critical nature. Include systems and applications developed internally (by Data Processing or by department members) and applications developed by external third party sources (consultant firms, etc.).

Description: ______________________________

Description: ______________________________

Description: ______________________________

Description: ______________________________

Description: ______________________________

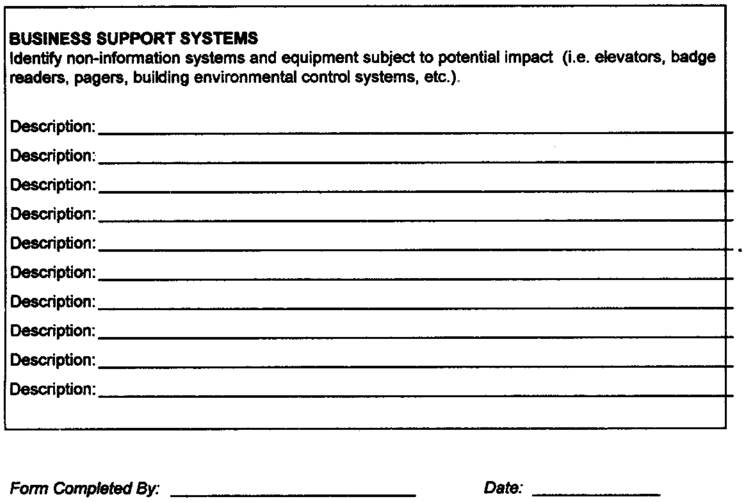
Description: ______________________________

Description: ______________________________

Description: ______________________________

Description: ______________________________

(Continued on back)



BUSINESS SUPPORT SYSTEMS
Identify non-information systems and equipment subject to potential impact (i.e. elevators, badge readers, pagers, building environmental control systems, etc.).

Description: ____________________

Description: ____________________

Description: ____________________

Description: ____________________

Description: ____________________

Description: ____________________

Description: ____________________

Description: ____________________

Description: ____________________

Description: ____________________

Form Completed By: ____________________ *Date:* ____________

CRITICAL SYSTEM EVALUATION

1. Critical System ID:

2. Critical System Name:

3. Task Assignee:

4. Owner:

5. Supplier/Vendor:

6. System Contacts:

Name	Organization	Responsibility	Telephone

1. System Description

1.1. Brief Description

1.2. Primary Functions

a.

b.

c.

1.3. System Type

[ ] Software System

[ ] Embedded Processor System

[ ] Non-Processor System

1.4. System Interfaces

Interface	Input	Output

1.1. System Operations

a. Does System Use Dates? [ ] Yes [ ] No

If Yes, describe how system uses dates:

b. Volume and Rate of System Transactions

[ ] High [ ] Medium [ ] Low

Details:

c. Critical Monthly Events

2. Non-Compliant Y2K Impacts

[ ] High [ ] Medium [ ] Low

Details:

3. System Unavailability Impacts (Emergency Conditions)

[ ] High [ ] Medium [ ] Low

Details:

4. *Software Systems*

4.1. Platform

[ ] Mainframe [ ] Workstation [ ] Server [ ] Other:

4.2. Operating System

[ ] DOS [ ] Windows 95/98 [ ] Windows NT [ ] Unix [ ] CMS/VSE [ ] VSE/VM
[ ] Other:

4.3. Language

[ ] COBOL [ ] NATURAL [ ] C, C+, C++ [ ] Visual Basic [ ] Other:

4.4. Software Size

a. **Number of Programs/Modules:**
b. **Source Lines of Code (SLOCS):**
c. **Other Measures of Size:**

4.5. Y2K Analysis

a. **Analysis Method**
Line-By-Line:
Tools:
Other:

b. **Remediation Methods**
Fixed Window/Year:
Sliding Window/Year:
Other:

4.6. Remediation Status

Program/Module	Percent Complete			
	Analysis	Updates	Unit Tests	System Tests

Program/Module	Actual/Plan Date Complete			
	Analysis	Updates	Unit Tests	System Tests

1.1. Is System Operational? [ ] Yes [ ] No

2. *Embedded Processor and Vendor Supplied Systems*

2.1. Certification of Y2K Compliance:

2.2. Plans for Y2K Compliance:

2.3. Test Reports for Y2K Compliance:

2.4. Status of Y2K Compliance

a. Percent Complete:

b. **Actual/Plan Date Complete:**

3. Risk Analysis

3.1. Risk Assessment

a. **Any Risks? [ ] Yes [ ] No**

b. **If Yes, Identify Risks:**

c. **Degree of Risk: [ ] High [ ] Medium [ ] Low**

d. **Probability of Risk Occurring: [ ] High [ ] Medium [ ] Low**

3.2. Risk Mitigation

a. **Method and Plan**

b. **Expected Results**

4. Comments

5. Recommendations

Y2K CERTIFICATION REQUEST

[Date]

[Manufacturer]
[Address]

Dear Sir/Madam:

Like most businesses, ***[Name of organization]*** continues to address the Year 200 issue. We are requesting a letter of certification indicating whether ***[product or service]*** is Year 2000 compliant. Our definition of Year 2000 compliant means the equipment will handle the date correctly now, at the turn of the century (Year 2000) and beyond (including leap years) and that date sensitivity is not an issue.

If ***[product or service]*** is not Year 2000 compliant, what steps are you taking to ensure that it becomes Year 2000 compliant? Further, what specific dates will the equipment, product or service be Year 2000 compliant and how will your organization validate compliance?

Thank you for your immediate attention and written response to this matter. We look forward to your immediate written response to this matter at your first opportunity but within 30 days of receipt of this letter. If you have any questions or concerns related to this request, please contact, ***[Name]*** at ***[Phone]***. Please mail all your correspondence to:

> ***[Name]***
> ***[Address]***

Sincerely,

[Name]

SAMPLE MITIGATION PLANS

COMMUNICATONS

SYSTEM	MITIGATION
Enhanced 911 system	Plan for degraded communication using other available systems.
Radio communications	Use backup power, if available. Plan to use alternate communication systems. Multiple units mean that the loss of one is not a major problem.
Telephone	Provide battery powered radio communication at every facility and for cellular phones. Instruct all personnel in its use and locations.

GENERAL SERVICES

SYSTEM	MITIGATION
Bank reconciliation systems	Continue to collect data from the bank with workstations running on backup power. Check with banks for their plans to retain data longer than two days if they experience Y2K problems.
Central accounting systems	Issue manual receipts. Manually process deposits. Provide personnel to process backlog.
Cost accounting systems	Consider manual processing. Prepare to work off backlog with additional resources.
General ledger systems	Ensure that system is Y2K compliant before June 30, 1999. Provide workstations running on backup power. Could manage up to a week manually, then significant backlog would result because of the high volume of transactions. Provide workstations running on backup power.
Payroll and personnel systems	Determine first pay date for 2000. Consider preprinting checks before the transition is being considered. Provide workstations running on backup power.
Billing systems	Produce hardcopy list of customers late in December to facilitate manual operation. Obtain additional personnel to enter backlog of data.

INFRASTRUCTURE

SYSTEM	MITIGATION
Backup generators	Plan for degradation of communications using devices that are independent of station power source. Provide adequate stand-alone fuel supply. Properly test ability of generators to provide backup power.
HVAC, heating and air conditioning systems	Use manual override or backup power, if available.
Public utilities	Install backup generators. Perform work manually, where feasible.
Traffic signals	Manual traffic control, if personnel available. Back up power source.

COURT OPERATONS

SYSTEM	MITIGATION
CLETS	Use backup power in event of a power failure.
Criminal case and court calendaring systems	Produce January 2000 calendars in late December. Revert to manual record keeping and processing. Ensure that adequate personnel are available to process manually and to handle any data entry backlog.
Jury systems	Prepare and print out January and February jury calls early.
Jail door controls	Operate manually using keys.

OTHER SYSTEMS

SYSTEM	MITIGATION
Lab testing system	Plan process and prepare hardcopy to facilitate degraded manual processing. Obtain additional personnel to enter backlog of data.
Welfare services systems	Use limited manual processing where possible. Backup power supplies. Provide additional personnel to process manually and to work down backlog when system available.
Permit tracking system	Issue permits and schedule inspections manually. Collect data for later entry. Use backup power supply.

Mr. HORN. I think it would be helpful for people in the hearing.

Mr. OSE. In case anybody would like to see what that looks like, it's the yellow book, actually pretty attractive. If you can get a copy and pass it to your colleagues, that would be great. But it will be entered into the record.

Ms. SMITH. We do have a few extra copies available, and it's also on the website—on the Merced website, the www.ca.merced.—wait a minute.

Mr. OSE. www.co.merced.ca.us.

Ms. SMITH. Thank you.

Mr. OSE. As far as the newest, largest city in the State, that means Citrus Heights, is it just happenstance that brings you to the fortuitous position you are, or are there things you've done in particular that we could share with other municipalities as far as an effort to be Y2K compliant?

Ms. CAPRIOLA. As I mentioned in my testimony, I think it is the timing. We don't have old systems. We don't have legacy systems that we're trying to create or bring up to date. In some ways it's an enviable position that we're in. And I would wish it upon everyone. But I think we've also learned from our colleagues who have gone through the process that's been articulated by State and Federal guidelines in terms of what we should be trying to do in trying to work with those service providers, Sacramento County and private firms that do provide a great deal of services for us, to make sure that the service delivery continues.

The one good thing, I think, that is coming out of year 2000 is that it's an opportunity for every organization to kind of step back and review what their technology systems are and it's kind of this crisis that's pushing us to get rid of some systems that need to be moved on; but change is hard, as we know, especially in large organizations. So I actually think that out of every crisis, including this one, there are very good things that are happening to our governments and to—so we become more entrepreneurial with better services and systems coming out at the end, though the process is painful and expensive.

Mr. OSE. Do you have anything else to add, Mr. Chairman?

Mr. HORN. Well, you're absolutely correct, and we've raised that question often in the hearings and a lot are doing exactly what you're doing, and that's the right thing to do. You can get rid of a lot of them or combine them or whatever, and this is the chance to do it.

Mr. OSE. Well, I would like to express the appreciation of Chairman Horn and myself for the testimony of the witnesses this morning. I know some of you have come quite a distance. We appreciate you participating. We're going to stay on this. One thing I hear everybody talking about is the interrelationship and the interdependencies between the Federal, State, and local, you know. We're kind of in this together so we need to keep working together.

So I again thank you.

With that, Mr. Chairman, I'd like to bring the second panel down. Thanks for coming.

Second panel is—we're going to take a short break here, but the second panel is Garth Hall with PG&E, Mike—is it Petricca?

Mr. LATINO. It's Tom Latino.

Mr. OSE. OK. It's Tom Latino with Pacific Bell, Roy Le Naeve and Steve Ferguson accompanied by Carol Hopwood. These will be largely utilities and service providers at the local level. So having heard from the State and local government, now we're into a new group.

Now I need to again swear everybody in.

[Witnesses sworn.]

Mr. OSE. Let the record show that the witnesses answered in the affirmative.

So, again, what we'll do here is we'll take testimony from the witnesses in total, and then come back with questions. We do request you go to the podium provided.

And with that, Garth you're first. This is Garth Hall with PG&E, the manager of their Y2K project.

STATEMENTS OF GARTH HALL, MANAGER OF Y2000 PROJECT, PACIFIC GAS AND ELECTRIC CORP.; TOM LATINO, PUBLIC SAFETY DIRECTOR, PACIFIC BELL, APPEARING FOR MIKE PETRICCA; ROY LE NAEVE, SENIOR PROJECT MANAGER, Y2K READINESS PROGRAM, SACRAMENTO MUNICIPAL UTILITY DISTRICT; STEVE FERGUSON, CHIEF OF INFORMATION TECHNOLOGY, COUNTY OF SACRAMENTO, ACCOMPANIED BY CAROL HOPWOOD, EMERGENCY MANAGEMENT, COUNTY OF SACRAMENTO

Mr. HALL. Mr. Chairman, members of the committee, I really appreciate the opportunity on behalf of PG&E Corp. to talk to you today. I represent the corporate program office across all the lines of business nationwide. You know PG&E, the utility. But the businesses nationwide, I assure you, have adopted and followed the same standards across the board that we have applied in utility, and I have been responsible in ensuring all of those things. I know that is of interest to you because of your national interest, but I will now focus up on the utility because that is the scope of the California hearing today.

Our program, of course, covers all of the elements that have traditionally been discussed and some of which you heard of today: The inventory process, the analysis process, the remediation, the fixing process, the testing, finally the certification process, and then the very important contingency planning process. All of those elements are very, very far along across our corporation and in the utility as well.

In July, we were very pleased to report to the North American Electric Reliability Council, which has received a charter from the Department of Energy, that we—for all the electric delivery systems in the utility—we are ready. So that means that anything that has to do with delivery of power to the consumers, we have assessed, we have fixed, we have tested, and we have certified. That includes, also, the power generation plants, the hydro and the fossil power plants that we still own, understanding, of course, that we have sold many lately. So all of those that we own in those domains are included in that. So that should be of enormous relief to those who have concerns about power, and we heard some of those reflected today.

In addition to that, we are very, very far along in the nuclear power area. We are down to less than 1 percent of items still in testing in the gas supply area and in the nuclear generation area at Diablo Canyon. There are very, very few, fewer than a handful of things, left in testing and certification of all those is expected in September. By November 1st, the California Public Utilities Commission requires us to file a written certification as to our state of readiness across all of our departments and functions in the utility. And we fully expect to file at that time that we are ready across the board, that everything is tested, certified and is ready.

Even though we are very confident about all of these things, we have also taken contingency planning very seriously. Every one of our mission-critical business partners, suppliers and government agencies has a contingency plan developed by us. In other words, for each one of those entities that we depend on to a strong degree for our ongoing continuation of business, we have already developed a contingency plan. Even when we are fairly confident, as with Pac Bell and many of the others that are represented today, that the service will be there and reliable, we still have developed a contingency plan.

In addition to that—at a higher level—we have developed business recovery plans that are really just continuations of our standard business recovery planning. As everyone would appreciate, we face storms, earthquakes, floods, during which power outages and gas line interruptions can occur. Our organization, having been trained and practiced in response to those, is the same organization that would have to deal with any type of high-level disaster whether driven by storms or Y2K or anything. Even though the probability of those may be very, very slight, we have drilled those internally twice in the utility now, making sure that everybody understands what they would have to do; and we have participated in one nationwide drill in April, organized by the North American Electrical Reliability Council, and we will do that again on September 9th.

We also recognize the importance of communicating our readiness out to the community, have met with over 100 various customer groups, including Hewlett Packard, Wells Fargo, Shell Oil, the Woodland Chamber of Commerce, many city councils, many county boards of supervisors, water agencies and trade groups. We will continue to do that. We understand the importance of communicating our readiness so people understand and have advice on how they should prepare. That's going to be an ongoing process for us.

With those remarks, I thank you again for the opportunity.

Mr. OSE. Thank you, Mr. Hall.

[The prepared statement of Mr. Hall follows:]

Year 2000 Readiness Disclosure

Testimony of Garth Hall

Program Manager, Y2K Program Management Office

PG&E Corporation

before

THE GOVERNMENT MANAGEMENT, INFORMATION AND

TECHNOLOGY SUBCOMMITTEE

OF THE HOUSE COMMITTEE ON GOVERNMENT REFORM

August 13, 1999

Sacramento County Board of Supervisors' Chambers
Sacramento, California

PG&E Energy Services, PG&E Energy Trading, PG&E Gas Transmission, and PG&E Generating are not the same companies as Pacific Gas and Electric Company, the utility, and are not regulated by the California Public Utilities Commission. Customers of Pacific Gas and Electric Company do not have to purchase products or services from these companies to receive quality service from Pacific Gas and Electric Company.

Good Morning, Mr. Chairman and Members of the Subcommittee. I am Garth Hall, Program Manager of the Y2K Corporate Program Office of PG&E Corporation. My office oversees and coordinates the Y2K efforts of all the Corporation's lines of business: Pacific Gas and Electric Company, the utility, PG&E Gas Transmission, PG&E Energy Services, PG&E Energy Trading and PG&E Generating. Thank you for giving me this opportunity to tell you about our program and its progress, and to support your efforts regarding the important issue of Y2K readiness. While the primary focus of this presentation will be on the utility, the same success story is true for our other lines of business.

I can assure you that we are taking Y2K seriously. We began our Y2K efforts in 1996. Since then, we have been working hard and committing the necessary resources toward resolving this issue.

Our goal is to have our mission-critical systems Y2K ready before the end of this year, and we are on target to do just that. As you probably know, the Department of Energy has asked the North American Electric Reliability Council, or NERC, to oversee the Y2K efforts of the nation's electric utilities to ensure electric reliability is maintained. Last month, our utility unit, Pacific Gas and Electric Company, reported that it is Y2K ready to NERC. Beyond reports to NERC, we also report the status of our nuclear systems to the Nuclear Regulatory Commission and Nuclear Energy Institute, and we respond to surveys about our gas systems to the American Gas Association. In NERC's final report, issued last week, NERC said it believes that "the electric power industry will operate reliably into the Year 2000."

We echo that sentiment throughout PG&E Corporation, and fully expect January 1, 2000 to be a day like any other day. To date, we have not found any Y2K problems that we have not been able to resolve. That being said, I also want to assure you that we fully understand the need to be prepared. Being prepared is at the core of our business – whether it is for storms, fires, earthquakes or Y2K. We are developing and testing comprehensive contingency plans. And we will continue various kinds of validation and quality assurance efforts into the new century to minimize the risk of interruptions of service for our customers.

Before taking your questions, I would like to briefly describe our Y2K program, contingency plans, and our public outreach program. We are addressing Y2K problems found in (1) software developed by our lines of business for specific applications, (2) software provided by vendors, (3) computer hardware and (4) embedded electronic systems. The first step of our program was to compile an inventory of all systems used, and to assess which systems are mission-critical. We purposefully concentrated our efforts on those systems that directly affect our safety and reliability, customers, products, and revenue. The utility depends on these mission-critical systems to deliver gas and electricity reliably and safely. Examples are those systems that provide outage information and monitor the transmission of gas and electricity, safety-related systems at our generating plants, customer billing and metering, and computer and telecommunications infrastructure that supports business operations.

Our plan calls for the remediation of any mission-critical system not Y2K ready. Remediation means that a system is either repaired, replaced or retired. After remediation, testing is performed to verify that the system will continue to operate into the next millennium. Certification, or the final step in our process, is to officially acknowledge that the work has been completed appropriately. Certification requires a review and formal sign-off by an officer of the company.

Another important component of our Y2K plan addresses mission-critical business relationships consisting of partners, suppliers and government agencies. We have assessed these relationships using Y2K compliance information obtained from them and, based partly on this information, have developed contingency plans for all of them.

We depend on these relationships, and if any of them experience Y2K problems, the reliability of our services may be affected. Indeed, the reliability of the entire electric industry hinges on its many interconnections and interdependencies. For example, to deliver power to utility customers, we are dependent upon the California Independent System Operator (ISO), which is located in Folsom. The ISO controls the operation of the State's electrical transmission system. The ISO is in turn dependent upon the proper operation of various transmission systems it is connected to throughout the western part of the US and Canada. Also, the utility sells to and buys power from the California Power Exchange, which relies on other many other power plants that must function properly to provide power needed at any time.

With the complexity of our industry and the physical nature of our utility system, it only makes sense to prepare for the unexpected. We are experienced in planning for contingencies; it's important to our business and service. Every year we prepare for the possibility of fires in the summer, heavy storms in the winter, and earthquakes that could occur at any time. We participate in emergency drills internally and with external agencies. We have existing plans and procedures in place for dealing with emergencies involving our gas, electrical, generating and trading systems.

We are building on these existing emergency plans in preparation for problems that may result from Y2K. We have been testing our plans and will continue to do so throughout the year. We are performing tabletop exercises with key personnel and training designated employees. In addition, under the direction of NERC, we participated with the ISO and other utilities in a nationwide Y2K exercise in April 1999 and will take part in a second exercise scheduled for September 1999.

Utility contingency plans for the Y2K roll-over period include: extra staffing at many of our facilities, operation of additional 24-hour call centers, emergency centers staffed and operational, and pre-scheduled transmission of additional gas and electricity. If gas or electric service interruptions occur, we will have personnel on hand to restore service as quickly and safely as possible.

We are committed to informing our customers and business partners about our Y2K plans, progress and contingency planning. We have a number of different avenues to communicate–from our regularly-updated Internet web sites and customer newsletters to face-to-face meetings.

Table of Contents

Purpose

Because of the nature of the electric utility industry, emergency response is an inherent part of Pacific Gas and Electric Company's daily operations. Many systems and procedures are already in place to deal with emergencies as they occur. The Y2K issue, however, presents an increased risk of simultaneous loss of systems and facilities that support our electric and gas lines of business. This increased risk warrants additional preparations and contingency planning by the utility industry to maintain safe and reliable service to our customers. Pacific Gas and Electric Company is making a substantial commitment of time and resources so that our information technology systems will continue to perform well into the next century. We are pleased to provide you with the following Year 2000 Readiness Disclosure information regarding Pacific Gas & Electric Company's Y2K contingency planning.

Scope

This document summarizes Pacific Gas and Electric Company's Year 2000 contingency planning efforts for power generation, gas and electric transmission, gas and electric distribution, information technology infrastructure (including communications, mainframe, and distributing computing systems), customer service and revenue-related critical operations. This document also provides a summary of the process used to assess critical business functions and determine the business units, internal and external systems, and business partner and supplier relationships that are critical to providing safe, reliable, and continuous service to our customers.

Y2K progress

Our efforts have been focused primarily on systems and equipment that are essential to providing safe and reliable service to our customers. As of June 1, 1999, we have completed our inventory, assessment, and remediation and are over 95% complete with testing. We have found nothing that would hamper our ability to be ready for the Year 2000 rollover.

Even if our gas and electric systems perform flawlessly, we depend on the reliability of other entities in today's energy industry. Pacific Gas and Electric Company is coordinating contingency planning efforts with its major business partners and agencies such as the California Independent System Operator (CAISO), the Power Exchange (CalPX), and the Western Systems Coordinating Council (WSCC).

The entire Y2K preparation process has been overseen by a steering committee of senior officers within the company. Steps that Pacific Gas and Electric Company is taking to ready itself for the Year 2000 rollover include:

1. Developing staffing plans to operate critical facilities during the Y2K rollover. Staffing plans have also been developed for computer and telecommunications specialists who support essential operating systems.

2. Developing a communication plan to educate employees, the public, and other constituencies about possible Y2K impacts.

Summary Contingency Plan

This section provides a summary description of Pacific Gas and Electric Company's Year 2000 contingency planning efforts.

Rollover period

The critical year 2000 rollover period will begin for Pacific Gas and Electric Company at 8:00 p.m. Pacific Time on December 31st, 1999 and will extend through 5:00 p.m. Pacific Time, January 4th, 2000).

The company will maintain its emergency management posture until such time as it believes that Y2K-related problems have been identified and resolved. It is expected that Pacific Gas and Electric Company's Emergency Operations Center will remain activated at least through Tuesday, January 4, 2000.

Emergency Operations Center and Operations Control Center Emergency Staffing

All company emergency centers will be staffed on December 31, 1999. The level of staffing will be commensurate with the nature of problems that may be encountered by a particular center. Pacific Gas and Electric Company will be in contact with the WSCC and NERC who will be monitoring events in other countries as the rollover occurs.

Company spokespersons will be available to respond to inquiries from the media and will be available for press conferences if needed.

Local emergency operations and governmental relations personnel will maintain contact with their respective County Offices of Emergency Services, Boards of Supervisors, and other local officials. The company will maintain regular contact with the CAISO, the State Office of Emergency Services, the California Public Utilities Commission, and other agencies as needed.

Grid Transmission and Generation

All critical grid devices and systems have been tested and will be certified to be Year 2000 ready. The majority of the devices and systems used to control and monitor the grid do not use date and time in their core or main function. Date and time function is primarily used for historical log stamping. There are some external risks which may impact service continuity. The most significant external risk is loss of generation. Since the CAISO has operational control of all the generating units, this issue will be addressed through joint contingency planning efforts currently in progress.

At our utility, we have responded by letter to more than 3,400 customer inquiries. Since February of this year, we have averaged more than 9,000 hits each month on our utility web site. Our media representatives have conducted nearly 250 interviews on this issue. Utility governmental relations representatives have kept elected officials apprised of our program.

The utility has taken part in more than 160 presentations throughout the service area, from San Francisco to the Sierra foothills, and from Redding to Bakersfield. Our audiences for these presentations have run the gamut – from corporations such as Hewlett Packard, Wells Fargo and Shell Oil, to the Woodland Chamber of Commerce; from city councils and county boards of supervisors to power and water agencies; and from trade groups, like the California League of Food Processors, to the Soroptimists in Auburn.

In closing, we feel we have implemented a strong and effective plan, devoted appropriate resources and diligently monitored the Y2K work throughout the Corporation. Though no one is able to predict with certainty what the Y2K transition will bring, we will be ready.

Thank you, Mr. Chairman, for inviting me to participate today, and I would be pleased to answer your questions.

Pacific Gas and Electric Company is working with the Western Systems Coordinating Council and other operating entities to develop mitigation and contingency planning strategies that will be implemented by all WSCC participants during the rollover period. Pacific Gas and Electric Company will comply fully with the WSCC plans, and has internal contingency plans that reflect the recommendations made by the WSCC for preparing for Year 2000. This section highlights contingency planning and mitigation measures Pacific Gas & Electric Company is taking to prepare for the Year 2000 rollover.

Staffing

Pacific Gas and Electric Company's staffing plans are in place and ensure that sufficient technical support staff will be available at control centers and related facilities to handle dispatch, scheduling, EMS, SCADA, communication, computer problems, etc. This includes operation engineers, additional transmission and generation dispatchers, transmission schedulers, EMS staff, system protection personnel, communication personnel, control personnel, network technicians, press liaison, management, programmers and other key support staff. Operational study personnel will also be available to evaluate impacts to transfer capability caused by loss of transmission and/or generation facilities.

Pacific Gas and Electric Company is prepared to augment its normal staffing plan with operation engineers, additional transmission and generation dispatchers, transmission schedulers, EMS staff, system protection personnel, communication personnel, control personnel, network technicians, press liaison, management, programmers and other key support staff beginning no later than 8:00 p.m. December 31, 1999 through close of business January 4, 2000.

Pacific Gas and Electric Company has identified 15 switching centers and approximately 70 critical substations that will be staffed with skilled operators and technicians prepared to assume manual control during the transition to 2000.

Pacific Gas and Electric Company will staff all of its generating plants with personnel trained and prepared to assume manual control if necessary.

System Posturing

In coordination with the CAISO, additional reserve generation will be available on December 31, 1999. Critical electric and gas facilities will be staffed so that the system can be operated in a manual mode if necessary. In the unlikely event that there is a problem with the CAISO's ability to manage the California electric system, the California Utility Distribution Companies (Pacific Gas and Electric in the North, and Sempra and Southern California Edison in the South) will be postured to run the electric grid self-sufficiently.

The company's initial focus will be on the viability of grid operating systems. Once the status of those systems has been determined, the focus will shift to financial systems and particularly those related to customers. If needed, essential financial functions can be shifted to a secondary location as part of the company's existing business recovery plan.

Prescheduling and Limiting Market Activity

Pacific Gas and Electric Company will comply with Y2K pre-scheduling limits assigned by the WSCC for key WSCC transmission paths. The Y2K scheduling limits are set to provide additional margin in the system to handle multiple contingencies. These limits will be in effect during the period 9:00 p.m. December 31, 1999 to 2:00 a.m. January 1, 2000. Note that there are two sets of limits, one for normal weather conditions and another for arctic express conditions in the Northwest. The WSCC will monitor weather forecasts and notify all operating entities on the morning of Tuesday, December 28, 1999 as to which scheduling limits will be used.

Update Operating Procedures

Pacific Gas and Electric Company is working with the Control Area Operator (CAISO) and other operating entities to coordinate contingency plans and to update the following operating procedures:

A. Load curtailment procedures
B. Operation without primary data and voice communication systems procedures
C. Black start and restoration procedures
D. Back-up control center procedures
E. Tie-line restoration procedures
F. Procedures for handling extreme light load or high frequency conditions
G. Cold load pick-up procedures
H. Operation without EMS procedures
I. Procedures for operation under islanding conditions
J. Back-up real time schedule cut procedures, for marketing entities, in case of voice and/or data communication failure.

Communications Satellite Phone Backup

Pacific Gas and Electric Company will have a satellite telephone in place in its Transmission Operations Center to communicate with the CAISO, which will have a link to the WSCC and NERC.

Gas Transmission

Gas Transmission specialists will be stationed at compressor stations and other gas sites during the rollover period. These specialists will be prepared to respond to gas transmission emergencies, including any possible Year 2000 problems

Nuclear Power Generation

The Nuclear Power Generation business unit has completed a thorough assessment of Y2K impact for the Diablo Canyon Power Plant (DCPP). In addition to remediation of plant systems, a comprehensive and detailed set of contingency plans was developed for plant systems and availability of key materials, consumables and vendor services. These Y2K contingency plans augment existing operating, abnormal operating and emergency procedures for DCPP. The Y2K contingency plans include staffing DCPP with additional key operational and management personnel during the century date transition.

Distribution

50 service centers will be staffed with gas and electric crews ready to respond to any type of distribution emergency, including any possible Year 2000 problems.

Customer Service

Pacific Gas and Electric Company's customer service call centers are the single point of contact for all customer inquiries and for civil authorities regarding trouble reporting. The communication systems, together with the call center specific systems are being thoroughly analyzed, tested, remediated where necessary, and will be certified as Year 2000 Ready.

The company will maintain its normal 24 x 7 schedule for call center staffing. We will also open an additional center with increased staffing. Other centers can be activated if needed. Call Centers will be open from December 31, 1999 to January 4, 2000, 24 hours a day, to respond to any problems that occur during the rollover.

Measure, Bill and Collect

Critical billing, measurement and collection systems will be monitored during the rollover. Specialists and technicians will be on site, ready to repair any possible problems.

Energy Bidding

Pacific Gas and Electric Company's Utility Electric Supply (UES) and Generation Portfolio Management (GPM) departments are responsible for bidding, scheduling, and dispatching electricity demand and generation into the market run by the California Power Exchange (CalPX).

UES and GPM do not have any physical assets or information technology infrastructure, but do have critical applications. Contingency plan strategies for both individual application failure and multiple concurrent application failures have been developed. If a system failure were to occur, manual bidding and standing bid procedures could be implemented.

Customer Billing

The billing processing systems and the credit and payment services systems, as well as the supporting infrastructure systems are being thoroughly analyzed, tested, remediated where necessary, and will be certified as Year 2000 Ready. Although the probability of failure is low, Pacific Gas and Electric Company has created robust contingency plans for its customer billing systems. Expert technicians will be on site during the critical rollover period prepared to resolve any problems should they arise.

Information Technology Infrastructure

Critical voice, data and computing systems will be monitored during the rollover. Specialists and technicians will be on site, ready to repair any possible problems.

General Services

Fleet

Garages will be open and staffed from 10 p.m. on December 31, 1999 to January 4, 2000, close of business. Garage personnel will be ready to respond to repair vehicles as needed.

All critical vehicles will be fully fueled prior to rollover.

Building and Land Services

Building and Land Services specialists will be stationed at key sites during the rollover period. These specialists will be prepared to address any building related problems. They will have vehicles and be prepared for dispatch to any site needing trouble-shooting.

Materials

Major materials distribution centers will be open during the transition.

These distribution centers will be staffed during the rollover period. Staff will be prepared to deliver critical materials and supplies to crews in the Pacific Gas and Electric Company service territory.

Emergency Plan Summary

Y2K contingency plans will be used as supplements to the company emergency plans and procedures.

Contingency Planning Process Summary

Year 2000 contingency plans were developed for Pacific Gas and Electric Company business units using a three-phased approach. The first phase produced a Category 1 contingency plan that identified the company's essential business functions and the business units that are responsible for supporting the various functions. The second phase required an in-depth assessment of the business units' functions and dependencies, and resulted in a Category 2 contingency plan. The third phase resulted in Category 3 contingency plans that address the systems and external business relationships that are essential to the function of the business units and therefore the essential business functions of the company.

The contingency planning process identified 245 essential systems to support the essential business functions of the company, 300 entities in the supply chain, and 331 business partners. Contingency plans were created for the critical systems, suppliers, and business partners. Category 3 contingency plans will be drilled continuously throughout the year. Organizations within Pacific Gas and Electric Company that developed contingency plans include:

- Generation Transmission and Supply (Power Generation; Electric Transmission; Gas Transmission; and Gas and Electric Supply)
- Nuclear Power Generation
- Distribution and Customer Services (Operations; Maintenance and Construction; Customer Service; Customer Revenue Transactions; Engineering and Planning; and Rates and Accounts Services)
- Computer and Telecommunications Services
- Controller
- General Services (Materials and Fleet, Building and Land Services)

Assess Risk of Failure of Essential Systems and External Entity Relationships

After essential business functions, their supporting systems and external entities were identified, the next step in the contingency planning process was to determine the risk level of each essential system and external entity. For the purposes of Year 2000 contingency planning, risk was evaluated using two measures: *probability of failure* and the *impact of failure*. A high or low rating was assigned to the probability of failure and impact of failure.

Consider Y2K Failure Scenarios

Each business unit has a strategy and a plan for dealing with Y2K-related failures.

The following are examples of Y2K failure scenarios:

- Loss of telecommunications systems;
- Loss of phone carrier system;
- Loss of computing network and subsequent shutdown of multiple key applications;
- Loss of material ordering system resulting in inability to provide emergency materials to field crews;

Multiple system failures are those that occur simultaneously. For each essential business function, failure scenarios were identified. If an essential business function contingency plan required addressing multiple failure scenarios, contingency actions were written for each scenario.

Contingency Plan Development

A contingency plan was developed for each essential business function (Category 1), each business unit-owned function that supports the essential business function of the company (Category 2) and all essential systems and external relationships necessary for the essential business function (Category 3). Templates were provided to facilitate the development of the plans (an example is attached as Appendix A).

Category 1 Company-level Contingency Plans

The company-level contingency plan identifies the essential business functions of the company, department ownership of these functions, key interfaces with external elements, possible failure scenarios, impact to the company, and response strategy and organization.

Category 2 Business Unit Contingency Plans

Category 2 plans identify the company's essential business functions and, additionally, identify the following attributes associated with these essential business functions:

- key interfaces with external elements
- dependencies with other business units
- most likely failure scenarios
- impact to local operations
- response strategy and personnel.

Category 3 Essential System and External Entity Contingency Plans

Category 3 contingency plans identify the essential systems, suppliers, and business partners (external entities) that support the essential business functions of the company. Category 3 plans provide detailed information needed for the business unit to respond to an essential system or external entity relationship failure, provide mitigation strategies, and define the actions that are to be taken by the system owner in the event of a system failure. Supplier and business partner Category 3 contingency plans provide mitigation strategies and detailed information needed for the business unit to respond to a Year 2000-related failure of the relationship between the business unit and any of the above-mentioned entities with which they have key relationships.

Create Essential System and External Entity Relationship Contingency Plans

After scenarios were developed, contingency plans for the essential business functions were written. Essential business function contingency plans in most cases reference individual plans for each critical system, supplier, and business partner supporting the essential business function.

Detailed contingency plans were written in a manner and format for ease of use in the event of an emergency.

The following list is a sample from the detailed Category 3 template:

- Name of the essential system and external entity, and the essential business function supported.
- Brief description of the functions or services provided by the essential system and external entity.
- Brief description of the impact to business operations and location in the event the essential business function is interrupted by loss of essential systems or external entity relationship.
- Brief description of the minimum service levels that must be achieved if the essential system or external entity relationship is disabled or degraded.
- List of the organization or response team that will, if necessary, be involved in triggering and implementing the contingency plan.
- Description of the criteria and procedures for implementing the contingency plan.
- List of related essential business functions from other business units with contact persons for each.
- Contact personnel for each essential system, supplier, and/or business partner (i.e., callout lists).
- Summary of the various failure scenarios.
- Summary of the various mitigation strategies for the failure scenarios.
- List of personnel and resources required to implement the mitigation strategies (high level).

- List of persons responsible (by job title) for implementing each step of the mitigation strategy for each scenario.
- Necessary changes to company policy to implement strategies.
- Expected life of plan.
- Damage control procedures.
- Criteria and procedures for returning to normal mode of operations.
- Contingency plan testing and exercises.
- Training.

Exercise Contingency Plans and Revise as Required

The North American Electric Reliability Council (NERC) directed a drill on April 9, 1999 and will conduct another on September 9, 1999. The NERC drills involve the entire United States including parts of Canada and Mexico. The California Independent System Operator (CAISO) is involved in the NERC drills both as a Security Coordinator for the Western Systems Coordinating Council (WSCC) and as the control area operator for the territory that includes Pacific Gas and Electric Company. The CAISO plans to stage several drills to ready itself and the entities within its territory for the rollover to 2000. The NERC and CAISO drills will test grid operations and therefore will require participation by Pacific Gas and Electric Company, in particular its Electric Transmission, Utility Electric Supply, and Generation Portfolio Management departments.

The Nuclear Power Generation department conducted a drill on May 6, 1999 and the Computer and Telecommunications Services (C&TS) department conducted a drill on May 26, 1999 to test contingency plans. Distribution and Customer Services (DCS) plans to conduct 18 individual drills to exercise contingency plans for critical Distribution Emergency Centers. In November, 1999, the Alternate Company Headquarters (ACHQ) will be activated to test Pacific Gas and Electric Company Company's gas and electric functions.

The Corporate Security Department - Emergency Planning Section coordinates contingency plan exercises and documentation for the Emergency Operations Center and supporting emergency coordination centers. Corporate Security facilitated Y2K "tabletop" exercises in March 1999 and will facilitate additional exercises in July, 1999. The July exercises will again enable multiple business units to meet with each other to test their contingency plans against various scenarios. The objectives for the tabletop exercises are to:

- Ensure that emergency plans are coordinated across the company
- Identify and resolve issues and strategies in advance
- Identify the appropriate Emergency Management Office level and staffing
- Educate and prepare key emergency management personnel

Reevaluate Contingency Plans as Assumptions or Risk of Failure Changes

The last step in contingency planning is to periodically reevaluate the plans if risks or assumptions change.

Quality Assurance

The Corporate Security department, Emergency Planning section has reviewed and provided feedback on Category 2 and 3 Contingency Plans.

Date:	
Revision:	
Plan No:	Category 3

Appendix A - Category 3 Template

-Essential System-

Year 2000 – Detailed Contingency Plan

Department:	
Essential System and Number:	
Category:	3

Plan Preparer:				
	Signature	Name	Position	Date
Plan Approver:				
	Signature	Name	Position	Date

Date:	
Revision:	
Plan No:	Category 3

Detailed Plan

Plan Section No.	*Item*	*Content*			
I.	**General Information**				
A)	**Purpose**	This Category 3 Plan is intended to outline detailed contingency plans that will be invoked by the Business Unit in the event that the named Essential System degrades or fails due to a Year 2000 event.			
B)	**Document responsibility**	The person who maintains the document, including the last revision date, its distribution and access.			
C)	**Information on Essential System**	Provide an overview of the key business functions of this Essential System.			
1)	**Provide the name of the Essential System and describe its function**				
2)	Direct impacts on business operations				
3)	Physical locations	(e.g., distribution operator's office, microwave tower, etc.)			
D)	Definitions	Definition of key terms and acronyms, and their interpretations/meanings specific to the Essential System. Include terms that signify a state of business/operation interruption.			
II.	**Plan Organization**				
A)	**Essential System Response Team (ESRT)**				
1)	Essential System Emergency Response Team Members	ROLE	NAME	TITLE	WORK PHONE NO.
		Lead			
		Alternate Lead			
		Member			
2)	Activation/De-activation of ESRT and communication to/from the ESRT – Person responsible	Name/contact information of person/alternate responsible for declaration of a disaster and activation / de-activation of ESRT. This person also communicates for and on behalf of the ESRT (usually a manager).			

Date:	
Revision:	
Plan No:	Category 3

Plan Section No.	Item	Content			
B)	**Acceptable Level of Operation**				
1)	Definition of the minimum level of acceptable operation for the Essential System	Define the minimum level of acceptable operation for each business process within/for the Essential System during an emergency such that if the level was not reached, then the Essential System's service can still be considered "available" (i.e. some processes may be able to stop temporarily, others may effectively operate at a reduced level).			
2)	Estimation of time sensitivity	Estimation of time sensitivity – how long can the business go without service from this Essential System before unrecoverable consequences occur.			
C)	**Incorporation of Related Essential Systems (Category 3)**	(There may be several Related Essential Systems)			
1)	Name and number of Related Essential System	Provide the name of the Related Essential System – Assumption is that the system's reliable functioning is absolutely necessary to ensure daily operations for this Essential System.			
2)	Estimation of time sensitivity	Estimation of time sensitivity – how long can the business go without service from the specific component before non-recoverable loss occurs.			
3)	List of Related Essential Systems and Contact Information	ESSENTIAL SYSTEM	NAME	TITLE	WORK PHONE NO.
		Lead			
		Alternate Lead			
		Member			
		ESSENTIAL SYSTEM	NAME	TITLE	WORK PHONE NO.
		Lead			
		Alternate Lead			
		Member			
4)	**Interdepartmental Coordination and Support**	Identify and verify your contact(s) within these support organizations should the need for their support arise. It is recommended you use existing day-to-day contacts whenever possible.			
	Materials - fuels, vehicles, etc.	Names, phone nos., fax, email, cellular, pager, etc.			
	Building - HVAC, generators, etc.	Names, phone nos., fax, email, cellular, pager, etc.			

Date:	
Revision:	
Plan No:	Category 3

Plan Section No.	***Item***	***Content***
	C&TS - voice, data, etc.	Names, phone nos., fax, email, cellular, pager, etc.
	Others as necessary	Names, phone nos., fax, email, cellular, pager, etc.
III.	**Management of Identified Risk/Failure**	
	These actions are followed until a failure is experienced or when it becomes evident that failure is imminent. After a failure has occurred, a decision must be made whether these actions should remain in effect, and switch over to "Failure Response". There may be several risks – each should be identified and treated separately.	
A)	**Risk/Failure Identification**	Define and describe briefly the situation which presents a critical risk/failure to the continued operation of the Essential System from Year 2000-induced events.
B)	**Risk/Failure Description and Impact**	Review identified risk/failure, determine potential failure modes and consequences, and document pertinent information.
C)	**Risk/Failure Mitigation Measures**	Use the information from event analysis to determine the mitigation strategies that will reduce the effect of a potential Year 2000-induced event. It may consider Year 2000 interdependencies. Mitigation strategies to consider may include: • implementing manual control for some of the operations • placing backup or standby systems in service • developing special procedures • monitoring systems to ensure proper operation • etc. Leverage existing procedures and practices when developing mitigation strategies.
1)	**Staffing Assigned:**	*An attachment to this template may be created or reference made to an existing emergency plan (refer to plan section and page).*
	Names	*Optional*
	Quantity	Determine partial/full staffing needs.
	Type of Classification	Identify positions; account for expertise needed.
	Shifts	Identify shifts and hours (period of time).
	Emergency Centers set up by noon on December 31	All emergency centers must be set up by noon and staffed by no later than 8:00 p.m.

Date:	
Revision:	
Plan No:	Category 3

Plan Section No.	***Item***	***Content***
	Duration (minimal consideration)	**Priority 1:** Friday, December 31, 8:00 p.m. - Tuesday, January 4, 5:00 p.m. Flexibility needed to accommodate staffing up/down. Please note that this is the **minimum duration required.**
2)	**Critical Location(s)**	Where will you assign employees?
	Field / Office site	Locations that are staffed to respond in the field or designated office(s).
	Emergency Centers	Location of emergency center(s) being staffed.
3)	**Communications:**	
	Internal (Pacific Gas and Electric Company) Communications	
	Phones/LAN	List phone, pagers, cell phones, home phone number, e-mail, fax. Create an attachment to this Readiness Plan identifying location and communications for positions being staffed. If this information currently exists in your department plan, reference specific sections and page.
	Radio	Prioritize Use Assignment - list with call signs NEXTEL assignment if applicable
	Satellite	Assignment - list locations and phone nos.
	Utility Emergency List	EOC Manual, section 10.0 (will be provided by Corporate Security by 12/1/99)
	External Communications:	List phone, pagers, cell phones, home phone number, e-mail, fax numbers for business partners, suppliers, vendors, governmental agencies, etc. (e.g., CAISO, PacBell, PX, BPA).
4)	**Temporary policy changes necessary to facilitate Risk/Failure mitigation measures**	E.g., HR policies, operating policies, etc.
IV.	**Failure Response**	
	These actions are executed depending upon which failure scenario is encountered, and a "disaster" is declared by the EMT.	
A)	**Failure Management Plan**	
1)	Objective of the Plan	For the scenario, document the intended outcome of the executing the plan (e.g., continue normal operations; continue degraded operations; abort the function as quickly and safely as possible; etc.).

Date:	
Revision:	
Plan No:	Category 3

Plan Section No.	*Item*	*Content*
2)	Resource Details for operating in contingency mode	List of resources / sources necessary for the smooth execution of contingency mode of operation (e.g., staffing, scheduling, materials, supplies, temporary hardware and software, communications, etc., with all the contact information).
	Food	Identify source for pre planned food service, phone numbers, delivery/pickup, billing, etc.
	Lodging	Identify source for lodging, phone numbers, billing, etc.
	Money	Augment petty cash/checking account and assign accountability and method for securing additional funds if needed.
	Security	Identify source for contract guard service, phone numbers, billing, etc. if needed. Identify contingency for card access system if applicable (contact Jeff Montana of the Purchasing Department for list of available outside security services).
	Reference Data	Identify need maps, diagrams, etc. and assign responsibility for providing as needed.
3)	Criteria and procedures for invoking and operating contingency plan	Briefly describe the event/trigger that would determine when the plan execution is initiated (e.g., experiencing serious system failures, missing a modification/re-work milestone, reaching a projected Year 2000 failure date, etc.). Also compile checklist of activities that need to be performed for commencement of contingency mode of operations (e.g., communications to staff, business partners, customers; Setting up of crisis center and help desk; invoking of all relevant emergency alternatives., etc).
4)	Criteria and procedures for returning to normal mode of operation	Define an event/trigger that would determine if the Essential System could revert back to normal mode of operations. Also outline a sequence of steps/activities that need to be performed for reverting back to the normal mode of operations (e.g., Communications to staff, business partners, customers; disbanding of crisis center and help desk; shutting-down of all relevant emergency alternatives., any post-contingency testing, etc.).
5)	**Expected life of the plan**	The time duration or the occurrence of another event which would indicate that the operations for the Essential System cannot/should not continue in the contingency mode.
6)	**Roles, responsibilities and authority of the contingency team**	Names, titles, contact information, roles, responsibilities/duties, status reporting, etc., of the members of the contingency team. During the pendancy of the plan, the team would act under the directives only from the EMT.
7)	**Damage control**	Procedures for recovering any lost/damaged data/transactions and relationships.

Date:	
Revision:	
Plan No:	Category 3

Plan Section No.	***Item***	***Content***
V.	Event Communications	
A)	**Event Communications**	**LOGS ARE REQUIRED** and will be part of the company's Year 2000 response documentation.
1)	Log	Identify the appropriate log form and assign individual/position responsible for logging significant steps in response, and key internal and external communications (some departments have log forms in place, which may be used here. If a department does not have a log form, Corporate Security can supply examples.
VI.	Training - Required	
A)	**Plan/Subject**	Summarize the training agenda/curriculum.
B)	**Individuals**	Identify those individuals trained by name, classification, date trained.
C)	**Trainer**	Identify who did the training.
VII.	Drills and Exercises	
	Departments may conduct exercises on their own to validate their understanding of the plan. Corporate Security will provide information for the EOC Tabletop Exercises only.	
A)	**Objectives and Scenarios**	Identify the scenarios/major issues and objectives of the exercise.
B)	**Individuals**	Document all departments/ sections represented, date of the exercise and names of those participating in the exercise.
C)	**Critique/Feedback**	Provide critique/feedback on lessons learned.

Mr. OSE. Mr. Latino.

Mr. LATINO. Good morning. My name is Tom Latino and I am director of the Public Safety Organization for Pacific Bell. I appreciate the opportunity to update you on SBC's readiness for the year 2000, and I'm happy to say that we have some great news to share. The bottom line is that when you pick up the phone on January 1st of the year 2000, our network will be ready to serve you just as it always has and so will the wireless, data, Internet, and other services which we provide.

We spent nearly 4 years preparing for this issue. As of June 30th virtually all necessary upgrades have been completed. A very few upgrades are scheduled to be completed by September. As we wrap up these upgrades, we will continue to focus on testing and finalizing our business continuity plans. All of our services will be tested and retested in simulated year 2000 environments prior to January 1st.

Our testing efforts also go well beyond our own network. SBC is working with the Alliance for Telecommunications Industry Solutions to test our services in conjunction with other communications companies and other industries. As a matter of fact, ATIS recently announced the successful completion of a Y2K test involving communication networks serving the credit card and financial industries. SBC and other communication carriers had no difficulty in transmitting financial data in a simulated Y2K environment. We have also worked closely with Telco Year 2000 Forum, which in December completed tests showing that local networks are prepared to provide uninterrupted service.

This internal and third-party testing provides further evidence that Y2K will be a nonevent for our customers. And while we strongly believe that that will be the case, we also recognize that factors outside of our control could potentially impact our services. To further ensure continuous quality service, SBC is enhancing its business continuity plans to prepare for Y2K contingencies. These plans are an extension of Southwestern Bell's existing procedures for providing service in the event of an emergency or natural disaster.

As part of these business continuity plans, SBC will increase staffing at customer support in business centers during peak periods leading up to and including the New Year's holiday weekend. We also are establishing command centers throughout our service territory to ensure a smooth transition to the new year. As you can tell, Y2K readiness has been a very big job. All told SBC has spent $200 million to prepare for Y2K. SBC's Y2K project management team is led by an officer of the company, and each of our major business units have dedicated Y2K coordinators responsible for managing year 2000 issues within their organization.

To keep our customers up to date on our progress, SBC's Y2K team maintains a comprehensive website with the latest information available. Anyone looking for detailed information on our Y2K readiness can access the Preparing for the Millennium Section of SBC's website at www.sbc.com. The site includes a selection that allows you to check on the readiness of the central office switch that serves your community. You can also register at the website to receive a copy of SBC's final readiness report.

Thank you again for the opportunity to provide this update.

Mr. OSE. Thank you, Mr. Latino.

[The prepared statement of Mr. Petricca follows:]

Y2K Update Presentation
Goal: 5 minutes

Good afternoon. My name is Mike Petricca, and I am Product Manager for Pacific Bell. I appreciate the opportunity to update you on SBC's readiness for the year 2000, and I'm happy to say that we have some great news to share.

The bottom line is, when you pick up the phone on January 1, 2000, our network will be ready to serve you, just as it always has. And so will the wireless, data, Internet and other services we provide.

We've spent nearly four years preparing for the Y2K issue. As of June 30, virtually all necessary Y2K upgrades had been completed. A very few upgrades are scheduled to be completed by September.

As we wrap up these upgrades, we will continue to focus on testing and finalizing our business continuity plans.

All of our services will be tested and re-tested in simulated year 2000 environments prior to January 1. Our testing efforts also go well beyond our own network; SBC is working with the Alliance for Telecommunications Industry Solutions to test our services in conjunction with other communications companies and other industries.

As a matter of fact, ATIS recently announced the successful completion of recent Y2K tests involving communications networks serving the credit card and financial industries. SBC and other communications carriers had no difficulties in transmitting financial data in a simulated Y2K environment.

We have also worked closely with the Telco Year 2000 Forum, which in December completed tests showing that local networks are prepared to provide uninterrupted service.

This internal and third-party testing provides further evidence that Y2K will be a non-event for our customers. And while we strongly believe that will be the case, we also recognize that factors outside of our control could potentially impact our services.

To further ensure continuous, quality service SBC is enhancing its business continuity plans to prepare for Y2K contingencies. These plans are an extension of Southwestern Bell's existing procedures for providing service in the event of an emergency or natural disaster.

As part of these business continuity plans, SBC will increase staffing at customer support and business centers during peak periods leading up to and including the New Year's holiday weekend.

We also are establishing command centers throughout our service territory to ensure a smooth transition to the new year.

As you can tell, Y2K readiness has been a very big job. All told, SBC has spent nearly 200 million dollars to prepare for Y2K. SBC's Y2K project management team is lead by an officer of the company, and each of our major business units have dedicated Y2K coordinators responsible for managing Year 2000 issues within their organizations.

To keep our customers up to date on our progress, SBC's Y2K team maintains a comprehensive Web site with the latest information available. Anyone looking for detailed information on our Y2K readiness can access the "Preparing for the Millennium" section of SBC's Web site, www-dot-sbc-dot-com.

The site includes a section that allows you to check on the readiness of the central office switch that serves your community. You also can register at the Web site to receive a copy of SBC's final readiness report.

Thank you again for the opportunity to provide this update.

Mr. OSE. Next Mr. Le Naeve. He's the senior project manager for the Y2K readiness program at Sacramento Municipal Utility District.

Mr. LE NAEVE. Good morning, Mr. Chairman, members of the committee. I am Roy Le Naeve, the senior project manager for the Sacramento Municipal Utility District's Y2K program. I thank you for the invitation to speak here today.

Sacramento Municipal Utility District, commonly referred to as SMUD, is a community-owned utility that services approximately a half million customers. We are the second largest community-owned utility in California and the fifth largest nationally. SMUD has 11 generating facilities with a maximum generating capacity of 1140 megawatts. Our purchase requirements ranges from zero to 1500 megawatts with largest purchases generally occurring during the summer months.

Our customer base includes some very influential entities such as the county seat, the Sacramento County, a major State prison in Folsom—Mr. Horn referred to prisons earlier—the California Independent System Operator located headquarters and their control center in Folsom, the Western Area Power Authority, also headquartered in Folsom, the Office of Emergency Services for the entire State of California, and the residing body and support locations for the State of California.

We clearly recognize and strive to meet our serious responsibility to provide a high quality of dependable and reliable power to our customers. At the outset of the Y2K project, SMUD recognized and respected the public's concern. We also understood that in spite of any eventual successes of overcoming the threat of Y2K problems, if those successes were not credibly presented to the public, a sense of personal concern would continue.

Consequently, as our project was put together, the task of communicating openly and frequently to our customers and the public at large was placed very high in our project plan. This has been achieved through a variety of processes such as news events, community forums, special media presentations, key account presentations, bill inserts, and the SMUD website. We believe the word is getting out.

Over the last 6 months we have seen a noticeable drop in what was previously widespread Y2K anxiety as SMUD is receiving less and less requests for Y2K information. We formalized our Y2K project in the late part of 1997 by inventorying all the items in the district that may be subject to Y2K anomalies, or the bug as you've heard of them. At the end of the inventory we placed each item in two major categories: mission critical and nonmission critical.

To date, we placed and prioritized more than 1,500 items onto the Y2K vulnerable list. Each of SMUD's inventory items have received reviews, evaluations, and in the case of mission critical items, serious testing. As of this date there are 35 items remaining on the list for disposition and currently undergoing remediation. SMUD has plans to remediate or replace all the outstanding items by October 1st, 1999. SMUD's Y2K efforts have enabled it to declare all of its 11 generating facilities Y2K compliant.

The year 2000 compliance for SMUD means that all mission critical systems have been tested for proper operation through the

1999 year and into the year 2000 timeframe. Further, where remediation actions were required, appropriate actions were taken. The systems were retested and no reasons are known to us that would preclude the system from performing into the year 2000.

To date, all the generation and distribution systems have undergone vigorous test requirements and they have been declared Y2K ready with minor exceptions by the North American Reliability Council. The exceptions deal with nongenerating requirements. For example, affluent meters are very important to us but are not important for the sake of producing electricity. As a point of interest, the meters in question had been made compliant and will be installed in our system prior to October 1999. Our Y2K project has received the highest possible organizational oversight from executive management.

As the Y2K project manager, I report on a weekly basis to an executive sponsor. On a monthly basis I brief and receive guidance from the entire SMUD executive team. Additionally, I brief and receive policy direction from our entire board of directors on a monthly basis. This practice is scheduled to continue well into the year 2000.

As Americans we enjoy the best and most reliable electric service in the world. While each utility plays its respective role, the high service reliability is achieved because of a network of utilities that have joined together to work together. The North American Electric Reliability Council promotes the reliability of the electric supply for North America and it oversees our Y2K activities.

Over the past months we have worked with NRC and the utilities to be ready to respond. In April we exercised all of our national and local communications capabilities to ensure that we could talk to each other under degraded communications capabilities. The next national exercise is scheduled for September 9th. The exercise is scripted to be a dress rehearsal for the night of rollover. We anticipate that much will be learned concerning our posturing activities in preparation for the new year.

In summary, SMUD offers no guarantee. We do a test. We have searched, evaluated, tested, reevaluated every vulnerable item known to us, and we're unaware of anything that would keep the lights from burning as bright on the night of rollover as they do today. Thank you.

Mr. OSE. Thank you, Mr. Le Naeve.

[The prepared statement of Mr. Le Naeve follows:]

YEAR 2000 READINESS DISCLOSURE

TESTIMONY OF ROY LE NEAVE
SENIOR PROJECT MANAGER, Y2K READINESS
HOUSE GOVERNMENT REFORM SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY
AUGUST 13, 1999
9:00 a.m.

Good morning, Mr. Chairman, and members of the committee.

I am Roy Le Neave, Senior Project Manager of the Sacramento Municipal Utility District's Y2K readiness program. Thank you for the invitation to speak to you today.

The Sacramento Municipal Utility District, commonly referred to as SMUD, is a community-owned utility that serves electricity to more than 500,000 customers in Sacramento County and a very small portion of Placer County. We are the second largest community-owned utility in California and the fifth largest nationally. SMUD has eleven generating facilities with a maximum generation capacity of 1140MW. Our purchase power requirement ranges from zero to approximately 1500MW with the highest purchases being required during the summer months.

Our customer base includes some very influential entities such as the county seat for Sacramento County, a major state prison in Folsom, the California Independent System Operator (ISO) headquarters and control center, the Western Area Power Administration (WAPA) headquarters, the Office of Emergency Services for the entire State of California, and the residing body and support location for the California State Capitol. We clearly recognize, and strive to meet, our serious responsibility to provide a high quality of dependable and reliable power to all of our customers.

At the outset of our Y2K project, SMUD recognized and respected the public's concern. We also understood that in spite of any eventual success at overcoming the threat of any Y2K problems, if those successes were not creditably presented to the public, a sense of personal concern would continue. Consequently, as our project was put together, the task of communicating openly, and frequently with our customers and the public at large was placed very high in our project plan. This has been achieved through a variety of processes such as news events, community forums, special media presentations, key customer presentations, special events, public board presentations, bill inserts and SMUD's web site. We believe the word is getting out. Over the last six months, we have seen a noticeable drop of what was previously wide spread Y2K anxiety as SMUD is receiving fewer requests for Y2K information.

We formalized our Y2K project in the late part of 1997 by inventorying all of the items in the District that might be subject to Y2K anomalies or "the bug" as you have heard of it. At the end of the inventory, we placed each item into two major categories—mission critical and non-mission critical. Of those categories we further established four priorities. The first three priorities fall within the "mission critical" category. Generation and acquisition of electrons is our number one priority. Distribution systems are priority two. Our revenue stream became priority three. Revenue stream includes our meters, accounting systems, billing system, and

YEAR 2000 READINESS DISCLOSURE

banking interfaces. Everything else became a non-mission critical function and thus a priority four.

To date we have placed and prioritized more than 1500 items onto the Y2K vulnerable list. Examples include telecommunications equipment, electronic meters and protective devices such as relays, breakers, and fault indicators. Each of SMUD's inventoried items has received reviews, evaluations, and in the case of mission critical items, testing. As of this date there are 35 items remaining on the list for disposition that are currently undergoing remediation. SMUD has plans to remediate or replace all outstanding items by October 1, 1999.

. SMUD's Y2k efforts have enabled it to declare all of its 11 power generating facilities Y2k Compliant, according to the definition set forth in SMUD's Y2k Project Plan. **Year 2000 Compliant** for SMUD means that all mission critical systems have been tested for proper operation through the 1999 year and into the Year 2000 timeframe. Further, where remediated actions were required, the appropriate actions were taken, the systems were retested, and no reasons are known to us that would preclude the systems from performing into the Year 2000.Please note at this point that any items or systems that were categorized as "mission critical" must be vigorously tested both individually and on an integrated basis before it can be signed off as ready/compliant . To date, all of the generation and distribution systems have undergone vigorous test requirements and they have been declared Y2K ready with minor exceptions by the North American Electrical Reliability Council (NERC) (Please see attached definition). The exceptions deal with non-generating requirements. For example, effluents release monitoring meters. Such meters are very important to us but have no effect on the ability of the plant to produce electricity. As a point of interest, the meters in question have been made compliant and will be installed in our system prior to October 1, 1999.

Our Y2K project has received the highest possible organizational oversight from executive management. As the Y2K project manager, I report and brief to an executive program sponsor on a weekly basis. On a monthly basis, I brief and receive guidance from the entire SMUD Executive Management team. Additionally, I brief and receive policy direction from the entire Board of Directors on a monthly basis. This practice is scheduled for continuance through the early part of the Year 2000.

As Americans, we enjoy the best and most reliable electric service in the world. While each utility plays its respective role, the high service reliability is only possible because the network of utilities that have joined together. The North American Electric Reliability Council (NERC) promotes the reliability of the electricity supply for North America and oversees the utilities' work on Y2k

Over the past months, we have worked with NERC and the utilities to be ready to respond. In April we exercised all of our national and local communications capabilities to ensure that we could talk to each other under degraded communications capabilities. We learned a lot about what we do well and some areas where we need improvements. Those improvements have been made and we now look forward to the next round of exercising in preparation for emergencies.

YEAR 2000 READINESS DISCLOSURE

The next national exercise is scheduled for September 9. The exercise is scripted to be a "dress rehearsal" for the night of rollover. We anticipate that much will be learned concerning our posturing activities in preparation for the arrival of the new year.

In summary, SMUD offers no guarantees. We do attest that we have searched, evaluated, tested, and re-evaluated every vulnerable item known to us and we are unaware of anything that would keep the lights from being as bright on the night of rollover as they burn today.

YEAR 2000 READINESS DISCLOSURE

DEFINITIONS

According to NERC's definition, "***Y2K Ready*** *means a system or application has been determined to be suitable for continued use into the year 2000.*"

Mr. OSE. Mr. Ferguson from the city of Sacramento.

Mr. FERGUSON. Thank you very much. My name is Steve Ferguson. I'm CIO information officer for the county of Sacramento.

Mr. OSE. Excuse me.

Mr. FERGUSON. On behalf of the county Board of Supervisors, I wish to welcome your committee and all of the witnesses today to our community.

On the Y2K issue, the county began addressing its Y2K issues back in 1995. In 1995 we formed a Y2K steering committee consisting of county executives and key business players. We began a formal assessment of our status risks and remediation alternatives at that time. Our Board of Supervisors has taken a very strong interest in this issue. They have made it clear to us that they expect to be informed on how the county is doing. In response to that, our first comprehensive assessment report was made to our Board of Supervisors in June 1998. Subsequently, we have updated the information of that report in February and the first part of this month. The Board has asked we give them a final readiness report in December 1999.

I thought I would take a few minutes to review a few of the key points that we've given to our Board that were identified in that report. The county of Sacramento plans to spend over $60 million in remediation of Y2K. While that may not be impressive at the Federal level or State level, it certainly represents a sizable investment for this community. There have been some big benefits out of that. No. 1 is we have used that investment. We have leveraged that investment to provide a technological foundation for the county's future. This foundation will help us provide better and more efficient community services in the future.

For example, we've upgraded our networks that will allow us to engage in e-commerce. We have upgraded our applications that will allow us to more interactively interact with our citizens in foreign e-government, and the IT work forces have had the opportunity to learn new skills.

The county is planning for a number of Y2K-related activities. We've been discussing some of the business continuity issues. We're also aware as provider of local services to a large community that we have public safety issues that have to be dealt with as well. We are planning the operation of a joint emergency operation center with the city of Sacramento over the millennium change, and we are planning numerous table-top exercises to prepare for what we expect to be a high level of activity due to celebrations around Y2K. We also realize we have a responsibility to communicate readiness to our citizens and our county public information officer has been very active in preparing a countywide public information campaign.

We've shared with our Board a number of concerns about our readiness in Y2K. I thought I'd just summarize those quickly for you. The first area of concern is the Family Support Bureau of child support issues. A recent failure in the State project has put the county at risk. We do not have time to remediate legacy systems in that area. However, plans are under way to implement a system, one of the four consortiums that was mentioned by your earlier testimony in the child support area, and that's planned to go live in November of this year.

Embedded chips, as others have mentioned, have been a major concern. The county operates numerous facilities from clinics to crime labs to jails and the airport, and we have been making major inroads in the testing and remediation of those types of issues. We believe most of that has been corrected and it will be operational through the millennium.

In the public safety arena, we've identified Y2K problems in our criminal justice systems. Pleased to report that just last month the Y2K readiness system went on line. The Sheriff's Department has identified Y2K problems with their computer-aided dispatch. They are now in the process of contingency planning should that system fail.

These problems, as I mentioned, are being addressed and we will continue to keep our Board informed on progress. A final area of concern that other members—other witnesses today have touched upon is the area of State interfaces. The county of Sacramento relies heavily on communication with the State of California. Myself and other CIOs throughout the State have expressed concerns repeatedly over the last few years about this, and I want to express my appreciation to Mr. Cortez, who has taken our concerns to heart and the State has renewed its focus in assisting counties in testing and working on those interfaces.

Again, thank you very much for the opportunity to testify today on behalf of Sacramento County, and we hope that your visit to the area is enjoyable.

Mr. OSE. Thank you, Mr. Ferguson.

[The prepared statements of Mr. Ferguson and Ms. Hopwood follow:]

Prepared Remarks for County of Sacramento, by Stephen R. Ferguson CIO

Congress of the United States
Committee on Government Reform
Subcommittee on Government Management, Information, and Technology
August 13, 1999
Sacramento, California

The County began extensive Y2K remediation efforts in 1997. These efforts include the replacement of our Financial/Human Resources/Utility Billing systems (COMPASS project), repair of our legacy mainframe systems (TAX and CJIS), numerous hardware upgrades to eliminate "embedded chip" problems, and many projects initiated by County departments on departmental business systems. As reported to our Board of Supervisors in December 1998, the estimated cost of these efforts will exceed $56.9 million.

County staff have reported the status of our Y2K efforts to our Board on a regular basis. Those reports included a comprehensive risk assessment compiled by an independent consultant. As confirmed by the consultant's assessment, the County continues to make excellent progress in dealing with known Y2K problems.

As of this time, the County's Financial, Human Resources/Payroll, Utility Billing, Criminal Justice (CJIS), and TAX systems are operational and Y2K compliant. A new Utility Billing system went live in late July 1999 and the final changes to CJIS were made in June and July 1999. Departmental systems remediation continues at an acceptable pace. At this time, we aware of only a few departments where higher risks still exist.

THE RISK ASSESSMENT

Carrera Consulting was hired under contract authority approved by our Board in December 1997 to conduct a comprehensive risk analysis. Carrera's assessment reports were presented to our Board in June 1998, February 1999 and August 1999.

The Board has adopted the consultant's recommendations that include the following:

- The County, through its Year 2000 Steering Committee, should follow up oversight of the Hot Spots.
- The County should continue the policy of centralizing all response to inquiries regarding Year 2000 preparedness through the Year 2000 Steering Committee
- The County should continue its Year 2000 Risk Management activities through its Year 2000 Steering Committee.
- The County should launch a Countywide Year 2000 Contingency Planning effort for Level 3 events. (Level 3 events are those outside of the County's direct control that

affect the lives of our constituents. These may include things like local business stopping operations, bank failures, etc.)

EMERGENCY RESPONSE PLAN

The City and County of Sacramento plan to open and staff an Emergency Operations Center (EOC) for this event. The EOC will be housed at the La Sierra Community Center located at 5325 Engle Road.

Emergency Operations staff are in the process of securing a backup generator for the center to ensure the operability of the EOC in the event of the loss of commercial power. In addition, we are working with telecommunications technical staff regarding the installation of a new phone system at the center. These two enhancements will be available and will be tested during our functional Y2K exercise scheduled for November 19, 1999.

A series of four tabletop exercises are planned for July and August. Each tabletop will include one of the functional core groups that will be working in the EOC during the New Years Eve period. Utilizing information gained from the four tabletop exercises, a scripted functional exercise will be developed and enacted on November 19, 1999. All of the EOC participants expected to be in the EOC on New Year's Eve will be trained during this exercise. Core groups expected to participate include Law Enforcement, Fire, Public Works, Energy, Utilities, Care & Shelter and Health Medical. Outside agencies will also be invited to participate in this exercise

Estimates of associated costs to outfit and activate the EOC are between $75,000-$150,000. There is a plan to share these costs between the County of Sacramento and City of Sacramento that are joint lead agencies in the Sacramento Operational Area.

The EOC is scheduled to open on December 27, 1999. We will be doing operational checks of all of the systems in the EOC during this week. The EOC will be activated at some level on December 30, 1999 in preparation for the New Year's Eve event period. Activation times and duration of the activation have yet to be determined. The EOC will be running on a 24 hour a day basis with two 12-hour shifts.

The EOC will be coordinating with other agencies such as American Red Cross, SMUD and other members of the Sacramento Operational Area during the New Year's Eve event in an effort to ensure that all agencies are kept fully informed as events unfold.

Y2K PUBLIC EDUCATION PLAN

The County's Public Information Office has developed a Y2K Public Education Plan designed to educate the County's constituents and employees on how to prepare to meet the Y2K challenge. This multi-faceted approach includes information on the extensive preparation the County has done to upgrade and/or replace vulnerable computer systems and bring them into Y2K compliance. We will also discuss our contingency plans that are designed to accommodate situations that may occur and how to minimize their effects; and common sense ideas on ways to be prepared in the event of temporary problems attributed to the Y2K challenge. The plan has five facets: a telephone hotline, a brochure, a Speaker's Bureau, a dedicated section on the County Web-site and a televised town hall meeting.

Beginning August 1, 1999, a telephone hotline number will be activated providing the public with 24-hours-a-day access to important Y2K information. Along with information regarding County Y2K efforts will be referral numbers for power and telephone companies, banking institutions, etc. The telephone number is (916) 874-2000.

The Sacramento County Sheriff's Department Office of Emergency Services has developed written information that has been compiled into a tri-fold brochure with the assistance of Vitali-Gage Communications, Inc. Entitled "Get READY, Get SET for Y2K," the focus is on separating fact from fiction regarding Y2K, and details the magnitude of the work the County of Sacramento has performed in order to bring its systems into compliance. Also included are some suggested tips for preparedness, how to reach our Speaker's Bureau, hotline and County Web-site, and where people can obtain more specific information, if desired. The goal is to both provide information and reassure the public with a common sense approach.

The Speaker's Bureau is comprised of high level Sacramento County employees assigned, by their Agency Administrators, to make presentations or answer questions at community group meetings. Requests so far have come from varied sources, including service organizations, hospitals and Y2K discussion groups. Speakers are selected in accordance with the type of information the community group is seeking, and can provide referrals to other sources for specifics that go beyond their area of expertise.

The County of Sacramento's Internet Web-site, which can be found at www.co.sacramento.ca.us, has a dedicated section devoted to Year 2000 information and preparation. Our required Readiness Disclosure can be found there, along with an Internet version of our written brochure and a wide variety of web-links to other resources on the Internet. It is one of the most effective tools due to the ability to update it frequently and reach a wide range of people.

Working in conjunction with the President's Council on Year 2000 Conversion, the County of Sacramento is hosting a televised town hall meeting this fall. Joining the federal "Y2K Community Conversations" effort, the goal is to bring citizens together with local business and government leaders to discuss readiness. The town hall meeting will include a host, a panel of experts and a studio audience. Working in conjunction with KOVR Channel 13, two independent producers are working with the Public Information Office to develop the agenda and guidelines for the meeting. In addition to reaching a large audience via KOVR, it will also be replayed on Channel 14, Access Sacramento and will be available to other commercial and cable stations. The County will also be web-casting the show, which means it can be viewed on the County's Website.

YEAR 2000 READINESS FOR SACRAMENTO OPERATIONAL AREA

What is Sacramento County doing to prepare for Y2K?

Sacramento County has been working on Y2K issues since 1995. Every department in the County has been independently assessed and is actively addressing its Year 2000 issues across all areas of concern including: Mainframe hardware and software systems
Embedded Systems
Critical Suppliers and
Contractual and insurance related issues

The County initiated two special projects for replacing large software applications with new systems certified to be Y2K compliant. Once project (Compass) replaced most of the County's financial, human resources, payroll and purchasing systems. The County's new financial system was successfully brought on line on July 1, 1998. The human resources and payroll portions were brought on-line December 20, 1998.

The second project (Focus) will replace the County's Utility Billing System. This system is due to be completed by the end of August 1999. Most departments completed their Y2K activities by the end of 1998. Those departments still working on Y2K issues are expected to complete their projects by the end of summer 1999, or to have work-around programs for those systems that cannot be made compliant by December 31, 1999. The County is currently focused on ensuring that all of its departments are ready to respond to any possible problems that might arise on December 31, 1999.

What Emergency Preparedness Plans are in place to respond to Y2K events?
The County already has extensive disaster response and recovery plans for natural disasters such as flood or earthquakes and these cover most of the potential problems that could be caused by year 2000 failures. The County plans to activate the Emergency Operations Center (EOC) on New Year's Eve. A small core group will be available to manage any issues that may arise. Law enforcement officers and staff in other departments have been notified that they must be available to respond if problems occur.

In addition, Emergency Operations is coordinating with the Sacramento Municipal Utility District, the Hospital Council, the California Grocers Association. Golden One Credit Union, The Sacramento Credit Union, the California Energy Commission and SouthWestern Bell, a parent company of Pacific Bell, to insure these entities are doing everything possible to insure continuity of their services to the general public.

When several million lines of date-sensitive computer code is reviewed and changed to be Y2K compliant, we believe the opportunity exists for errors to occur. We believe that we may have some disruptions from time to time, but overall we believe that our citizens will have electricity, water, and phone service when they need it. Because of the potential for some service disruptions, we believe it is prudent for our constituents to set aside a few supplies. Citizens should prepare for Y2K using similar steps as they would for any potential emergency.

What people can do to be prepared
Check with manufacturers of computer-controlled electronic equipment in the home to see if that equipment is affected by Y2k. This includes fire and security alarm systems, programmable thermostats, appliances, consumer electronics, garage door openers, electronic locks, and any other electronic equipment controlled by an embedded chip.

Keep a stock of supplies on hand. Enough to last three days to a week for every member of the family. Don't forget the family pets. This includes non-perishable foods, stored water and a supply of prescription and non-prescription medications that people use regularly.

Have some extra cash on hand (Traveler's Checks). Enough to last a week or two, in case ATM and credit card transactions are not working.
Keep the gas tank full.
In case there is a power outage, citizens should plan to use an alternate-cooking device.
Open flames or charcoal grills should never be used indoors!
Have flashlights and extra batteries on hand.
Store one gallon of water per person per day. Store water in sound plastic containers. Boiling water before use is the safest method of purifying water, but also have a water purification kit on hand. To boil water, bring the water to a rolling boil for 1-3 minutes. Other water sources in the home can be found in ice cubes, canned fruits and vegetables or in the reservoir tank of the toilet (not the bowl).
Store non-perishable food items such as: dry and canned goods, soups, juices, milk, beans, rice, boxed foods, vegetables and pasta.
If a power failure occurs, use perishable and refrigerated foods first and then foods from the freezer.
Also have a manual can opener and utility knife available.

Prepare a Go-Kit
Prepare a Go-Kit with essential supplies and copies of important papers in case you need to relocate during a prolonged power outage.
Keep items you would most likely need in a backpack or duffel bag and keep it handy.
Items to include in the Go-Kit: toiletries, snacks, a mess kit, a change of clothes, shoes, a book or games, important family documents, and a battery-operated radio.

Simple steps to take to protect family and property

- Learn first aid and have a first aid kit in the house
- Know where the utilities are located and how to turn them off
- Check insurance coverage-Know what insurance does and does not cover
- Plan ahead. Discuss family evacuation plans.
- Teach children how and when to call 9-1-1 for emergency help. Know who your neighbors are and who needs help during an emergency.
- Keep copies of important documents in a safe place. Use safe deposit boxes to store insurance and home mortgage information.
- Listen to news and weather reports. The Emergency alert station in our area is KFBK radio 1530 am.

What can citizens do to help in the community in the event of disaster?
Citizens can volunteer at a number of community based organizations
American Red Cross: 368-3131
Salvation Army: 648-3012
Volunteer Center: 567-3100
Info Line: 498-1000

What other jurisdictions are doing to prepare for the Y2K event

Cities within the geographic boundaries of Sacramento County have all gone through a process of inventorying their computer systems and equipment that utilizes embedded chips. All have repaired, replaced or retired these systems and components. Water districts have also gone through this process and are in good shape relative to their water capabilities. Our local utility companies also report that their processes are on time for the upcoming Y2K period.

Other contacts with local banks and grocers reveal the same attention to detail as noted above. All business sectors are doing everything in their power to ensure that their services will be available during the Y2K rollover.

Mr. OSE. Mr. Chairman, would you like to proceed?

Mr. HORN. Wonder if Mr. Willemssen could join us at the table. He's our all-around expert in Washington for the General Accounting Office. It's part of the legislative branch.

Mr. OSE. Without objection.

Mr. HORN. We always like to hear what he says. He's been to I don't know how many States now, but if he's putting pins on them, I think he will hit about 50.

Mr. LE NAEVE. Does he have easy questions?

Mr. WILLEMSSEN. Sometimes.

Mr. OSE. It's the answer we're after, Mr. Le Naeve.

Mr. HORN. Go ahead. What's your reaction now? You've heard the whole second panel, you've heard the first panel.

Mr. WILLEMSSEN. I thought you might want to followup on a couple of things that Mr. Hall and Mr. Le Naeve pointed out just to confirm the August 3rd, 1999 report of the North American Electrical Reliability Council does identify Pacific Gas & Electric as Y2K ready and does identify Sacramento Municipal Utility District as ready with limited exceptions, as was testified to. The report also notes 84 percent of the Y2K programs of all these bulk electrical suppliers have been audited and reviewed, some of them by internal auditors, some by external reviewers. It does not identify which ones have had those kind of reviews. You may find it useful to ask the witnesses today if they've had independent verification and validation reviews and if those reviews are—the reports of those reviews are publicly available.

Mr. HORN. That's a good question. I also would wonder, on that report by the council, is there any difference in terms of the state of analysis and surety between the nuclear and nonnuclear reactors.

Mr. WILLEMSSEN. There is a distinction made, and I believe the latest data on nuclear facilities indicates that there are approximately 35 such facilities that still have some exceptions that are being aggressively dealt with.

Mr. HORN. Because you know the Nuclear Regulatory Commission has told us they were going to do a 10 percent audit. We objected and said, "Why don't you do 100 percent?" And they objected, and said, "You don't understand what we're doing." And I said, "Fine. Put it in writing." I don't think I've still heard from them in writing. It helps hone the mind when you get them to put it down on paper, but I was curious what's happening in that area.

You heard the question. I just wondered if you have any thoughts in response to Mr. Willemssen's point.

Mr. HALL. Let me speak for PG&E. On the August 3rd report by the North American Electrical Reliability they were correct, in referring to PG&E, that they reflected our report to them that our electric delivery systems were totally ready. In other words, our systems are tested and certified.

The question about Diablo Canyon, which is our nuclear power plant, I'll just focus on that. That's 1 of the 35 that were reported to the Nuclear Regulatory Commission as having limited exceptions. It has one, and that will be in place and certified by September. The NRC, of course, is watching things very closely, and we are very diligently working with them. In terms of audits, the

NRC, in terms of the contingency planning arena, selected six plants nationwide, to my best knowledge, one of which happened to be Diablo Canyon. Diablo Canyon was audited by the NRC very exhaustively in terms of its readiness for handling emergencies in terms of contingency plans, and we have the report on that. That was very favorable. To my best knowledge, it's available to the public at the NRC's website. It's a publicly available document.

If I missed anything, please followup.

Mr. HORN. Anyone else like to comment on Mr. Willemssen's question?

Mr. LE NAEVE. I would just comment about the auditing of our project. Our auditing department works specifically and directly for the general manager which bypasses about 10 levels of the bureaucracy, if you will. There are three full-time auditors that I call them the truth sayers. They don't work for me, which means that they make me tell the truth. Two of them are SMUD employees, and the other is an outside auditor. In terms of being ready with exceptions, the rules are always a little sticky. Our plants, as I have testified, are very capable tonight to generate everything that it's supposed to generate. The meters, they're affluent monitoring meters that we need that data in order to report the types of pollutants that are going into the air and they meet with Federal standards and State standards but they have nothing to do with the generation capability.

Mr. HORN. Any other thoughts, comments, anything else from the General Accounting Office?

Mr. WILLEMSSEN. I felt one thing that you have asked at prior hearings and especially in terms of counties is when they had actually started their Y2K efforts. The year that the county started in 1995 is generally much earlier than what we've heard in other jurisdictions throughout the country, so I think that's worth noting.

I also think it's worth noting what the county mentioned in terms of its plans for additional table-top contingency plan exercises, no matter what good of shape they are in because so much is outside of their control, I think that is a worthwhile effort to pursue.

Mr. HORN. I guess I'd ask this panel, what is the sort of continuity and fallback plan that you have? For example, the Federal Government when we ask them, "Where were your contingency plans?" And most of them said, "Oh, we're depending on the U.S. Postal Service." So we held a hearing with the United States Postal Service, and it turned out they didn't have a contingency plan. So if something is falling through the cracks, how do we solve that problem with the utilities?

Mr. HALL. Did you want to go first?

Mr. LE NAEVE. In our case we are mandated by NRC. If not just a prudent action, we have contingency plans that takes into account our worst-case scenario as well as our worst-probable scenario and those contingency plans basically means we operate our system manually and we exercise accordingly. But to my knowledge, we have a contingency plan for just about any eventuality, not the least of which is Y2K. In the case of Y2K, we certainly don't expect any structural damage, which is what we typically have during storms. So I believe, speaking certainly for SMUD, we have contingency plans in place and we exercise them.

Mr. HALL. As far as PG&E, in addition to the remarks I made during my testimony about that, over the New Year weekend for a period of 4 days solid, we will be activating to the highest level of preparedness our emergency operation centers, which really places additional staff operating people in the field and at all key places and at the central location. Even though we don't expect anything to happen, we want to make sure everybody is prepared and ready, and the preparedness of those people goes very deep in terms of the activities they would have to undertake.

It also does include, by the way, invitations and close links with OES, Office of Emergency Services, directors from the counties and from the State who are tied into our distribution emergency centers. And so are the police force and fire station links. That's where the linkage occurs. So the good part of this is for emergencies unrelated to Y2K, those practices and infrastructures and procedures are in place.

What we're doing with Y2K is just bringing them up to a level where everybody is there, ready, in case anything happens, which we do not expect.

Mr. HORN. Well, it's like Jeopardy. You answered the question before I asked it. I'm curious because in some States we find there's a lack of frequencies where they can communicate. There is just overload, and we had that in L.A. County about 10 years ago where none of the police departments could talk to the Sheriff's office or anything else. And they've remedied that. They needed some more frequencies. So I take it it's not a problem for you, where you operate. You have what, two-thirds of California, at least?

Mr. HALL. Approximately so. Frequencies—apart from depending on Pac Bell, we have our own internal telephone network which covers the entire area independently. We also are relying on radio, and we also will be having satellite telephones as backup in a few key locations if everything else fails, including Pac Bell, which we do not expect.

Mr. LATINO. Mr. Congressman, Pacific Bell certainly will be ready. Business continuity plans are in place. They have been socialized with the appropriate support personnel and those systems that require those plans will, in fact, be fully staffed. We will have plans to activate our command centers as well as our network operation centers. Once again, they will be fully operational as well as fully staffed.

Additionally, specifically as it concerns public safety, we will have knowledgeable personnel in the field at key public safety sites in order to assist in any identification, isolation and resolution of trouble. Moreover, we will have established a command center for our 911 infrastructure itself.

Additionally, we have worked extensively with our 364 public safety answering sites in order to ensure they take steps to have contingency plans in place such as alternate answer. And last, we have worked closely with our directory assistance in the event, the unlikely event, of a 911 failure where seven-digit emergency numbers could be communicated to the public.

Mr. HORN. Interesting.

Mr. LE NAEVE. I'd just like to say we are in exactly the same situation. We typically have 2,500 employees. That night 20 percent of those folks will be up and running and in their office and in their locations both in our emergency center as well as our energy management center as well as manning our key bulk substations, which are things we typically would not do just in the eventuality that something happens.

Mr. HORN. Does SMUD have the natural gas as one of its products?

Mr. LE NAEVE. We are a purchaser. We don't produce any—matter of fact, Mr. Hall's company produces and issues most of our gas. We don't deliver gas to anybody.

Mr. HORN. Reason I ask that, in Eastern Europe and Central Europe we have a major natural gas problem where most of that is supplied by the Russians and through either pipeline or ship; and this is, of course, January, and it could be if that can't get through that or is utilized or leakage or whatever, you would have most of Eastern and Central Europe freezing pretty badly. Because if it was a Y2K affair that triggered something—and we know that there are microchips involved in the refinery and in the ships that haul that's under compression and so forth. So we don't have that problem here?

Mr. LE NAEVE. Not at SMUD.

Mr. HORN. OK.

Mr. FERGUSON. If I could comment on the county's preparedness contingency planning. Like any other local government in California, we have considerable experience responding to natural disasters. With one exception, the county is preparing for Y2K similarly to prepare for any other disasters that's also our flood season here. So we're prepared, the exception being that, and we've discussed this at great length, many times, the response of natural disaster depends upon mutual aid between governmental jurisdictions. We realize at this point that this problem could be very widespread. So we're not counting on mutual aid in our preparations.

Mr. OSE. If I may inquire, Mr. Ferguson, as it relates to the airport, December 31st is typically a pretty heavy travel day. As it relates to the airport operations, what, if anything, has the county—how has the county interfaced or interacted with FAA or operations at the airport to ensure that an unlikely contingency can be handled out there, that being the system goes down for either an unfortunate lack of power or an imbedded chip failure or something of that nature?

Mr. FERGUSON. Well, the rest of the—fall into three categories. Businesses, which I briefly addressed in my responses, to the extent they need to get bills paid and payroll out.

Second area is in the imbedded chip area. These are systems that run the airport, everything from the parking tickets dispensing system and fuel dispensing, et cetera. We assisted the airport. They've done a very good job in evaluating those imbedded chips and we have a program under way.

Third area of risk, we call this retractable kinds of risk. To the extent that the airport depends on the Federal Aviation Administration to control traffic, we have no opportunity to deal with that. It's just something we depend on someone else to provide as well as with the airlines. They have their own major business systems that run their reservations ticketing operations. And we are relying on them, as we are at the FAA, to deal with their Y2K risks. All reports we have at this time is that they are making good progress.

Mr. OSE. You're confident about the county success rate of progress to date on the systems that they have authority over or responsibility for?

Mr. FERGUSON. I would say the county is—it's at the 90 percent rate in terms of remediation across the board at this point.

Mr. OSE. Are you going to be at 100 percent come the first of the year? That's the question.

Mr. FERGUSON. Probably 99.99 percent. There are obviously going to be a few areas we miss, a small computer in a remote office, but we don't expect that to have any impact on our business operations.

Mr. OSE. I want to visit on one other aspect of this. SMUD has a website?

Mr. LE NAEVE. I'm sorry, sir?

Mr. OSE. Does SMUD have a website?

Mr. LE NAEVE. We do.

Mr. OSE. OK. And Pacific Bell has a website?

Mr. LATINO. Yes, sir.

Mr. OSE. And PG&E has a website?

Mr. HALL. Indeed, we do.

Mr. OSE. And I'm curious whether or not on any of those websites, in the unlikely event of a failure wherever, your subscribers, your ratepayers, or your service recipients could access those websites for contingency alternatives?

Mr. LE NAEVE. In our case, Congressman, that whole website issue is being discussed as it is and will continue to be right up to the night of rollover. We're getting several reports from the FBI and a few other places of criticality of people coming in and getting into our system and attempting to bug it, if you will. And getting into our system of direct path is through our website. We are toiling—emphasize the decision has not been made—but we're toiling with the possibility of shutting that website down for a few hours before and a few hours after the actual rollover.

Now, should the disaster happen that we've all heard about, clearly we would expect to communicate either through the National Emergency Broadcast System or some other means to get the word out as to what we're going to be doing. We will be in constant contact with the county. They will be in contact with us, and we would look to the county and to the State to assist us in getting out whatever word we need to. But to tell this committee that we are going to guarantee that they can access our website, I'm unable to do that.

Mr. OSE. I'm more interested in, say, between now and 11:59 on December 31st, posting information on the website in your respective organizations in the event of X——

Mr. LE NAEVE. We do that, yes, sir.

Mr. OSE. Pacific Bell do that and PG&E?

Mr. HALL. We have some guidelines and questions—typical key questions and answers that have been asked—for public information, but it is an idea that I want to take back with me and pursue a little more. I think there is some more merit in that idea that we haven't pursued all the way. I think especially approaching the year end timeframe there may be a subset of our customers that might choose to look first there. So I'm going to take that back and take a closer look at the opportunities for that.

Mr. OSE. It would seem to me even if the websites—in order to shut off access from someone trying to hack, even if the websites are shut down at least between now and then, people can print out or pull down off the web these very suggestions and print them out and keep them readily available.

Mr. LE NAEVE. We do that, Congressman, even to the point of the use of portable generators, which is a big fear that the average person would attempt to use a portable generator and without some basic knowledge and understanding all they do is get into a self-destruct mode. So we use our website to get that type of information out as well and to caution them for the proper usage as well as the most common asked questions. There's a shred out to our website that is Y2K specific and we update that at a minimum on a monthly base.

Mr. OSE. As a representative from a rural area, you can understand my concern. Many of my people have livestock that require regular water and regular feed.

Mr. LE NAEVE. Sure.

Mr. FERGUSON. If I may just briefly comment on the county's website efforts. We, too, have a website. However, we are aware that we serve all the constituents of Sacramento County, many of which may not have access in their homes to Internet technology. So our program is multifaceted and involves a public information campaign, town hall meetings, and actual written material that we're mailing out in our utility bills to try and get exposure to the broadest level of our constituency.

Mr. OSE. Now, there's a date coming up in September, September 9, 1999, which I'm familiar with, but would anybody care to briefly explain what that date comprises? It's a virtual equivalent in some instances to the December 31, 1999 rollover.

Mr. FERGUSON. I think that's something that's been overexaggerated a little bit. Commonly in the old days programmers used a collection of nines perhaps to represent the end of a file or some other condition. Fortunately, I think most computers would represent that date as September 9, 1999. So it's unlikely it will cause some of the predicted failures that people have talked about. But in all of our remediation efforts of our legacy systems, we have examined that as well as other Y2K-related issues. There's a date coming up in February 2000 which would be the first leap year date after the change of the millennium, making sure that is corrected as well.

Mr. OSE. Some of you have actual tests going to transpire on the 9th of September?

Mr. LATINO. Pacific Bell, Congressman, is continually ongoing in their testing requirements. Specifically in relation to September 9, 1999, we have prepared a separate business continuity plan for that day where we will have people staffed at our critical systems, and I'm addressing specifically our 911 system. And we have a scheduled list task to be performed in order that the right metrics can be evaluated to ensure that processing is going as expected.

Mr. LE NAEVE. In our case, the reason NRC decided to play the national exercise on September 9th was precisely for that reason. That puts all the required forces in the utilities in the right place in the eventuality that something did happen.

Mr. HORN. Mr. Latino, it's good to hear that Pacific Bell's 911 lines will operate. Isn't there a problem here with the people that are taking those calls? Most of them are either law enforcement or established by city managers, however, and how vulnerable does that make—you might have a good capability, but what's the human element here?

Mr. LATINO. Certainly the human element here is to make sure that there is not miscommunication, and toward that end, we have really launched an extensive effort in 1999 to communicate with our public safety partners. We've done this through numerous letters indicating the status of their equipment that we, in fact, provide and the need for them to check with other systems that we do not have responsibility for. We have participated in over one dozen forums, both with the public as well as with public safety personnel. We have sent out bill notices and inserts to further communicate the status of the 911 infrastructure concerning Y2K. And just as we said, we have distributed this to every public safety agency in the State that we supply which is, once again, our cookbook on how prepared we are for Y2K with 911.

Mr. HORN. If you could submit that for the record, maybe we can get a lot of it in the hearing.

Mr. LATINO. Yes, sir.

Mr. OSE. Without objection.

[NOTE.—The publication prepared by Pacific Bell entitled, "Pacific Bell Public Safety Solutions" is retained in the files of the subcommittee.]

Mr. OSE. Now, before I go on with my other questions, I want to get the website addresses each of you have in the record. It's www.smud.com and www.sbc.com?

Mr. LATINO. Yes, Mr. Congressman.

Mr. OSE. www.pge.com.

Mr. HALL. Right. And I just emphasize that's "pge" without the "&."

Mr. OSE. Right. Just the letters, no ampersand.

Mr. LE NAEVE. Sorry, sir. You said SMUD dot—ours is org, o-r-g.

Mr. OSE. www.smud.org in your case?

Mr. LE NAEVE. Yes.

Mr. FERGUSON. And the county's website is www.co.sacramento.ca.us.

Mr. OSE. Sacramento all the way out.

Mr. FERGUSON. Spelled.

Mr. OSE. All 10 letters.

Mr. FERGUSON. It's a mouthful.

Mr. OSE. Couple of other questions, if I might. I know PG&E receives some gas from foreign sources, that being Canada, and Pacific Bell is going to receive calls from overseas presumably, and SMUD perhaps by wheeling may receive energy from Canada, either through WOP or otherwise. Are there challenges each of you face in interacting with companies that might not be Y2K compliant and how are you dealing with those?

Mr. HALL. You mentioned PG&E first so I'll respond first—and we also include gas from Texas.

Mr. OSE. That's a foreign country, too.

Mr. HALL. That's a foreign country to us, indeed. But to be frank, initially the Canadian utilities were not under the same freedoms or onuses to reveal the status of their programs as their U.S. counterparts were, and so we initially had difficulty obtaining valid information as to where they were going and where they were.

That has changed. And we have derived—and our affiliates who actually transport the gas from the Northwest have derived—very good information and have participated in several face-to-face meetings where a substantial amount of readiness information has been shared—to the point where we are very comfortable that they have taken it seriously. They'll be ready.

So I think at this point we see both from the Texas side and from the Canadian side that we do not see any issues there that we can identify right now.

Mr. LATINO. Congressman, if I may add, our corporate headquarters is in Texas. So we have a very good relationship with that particular foreign country. And certainly we are testing internally. There are two key forums from the telecommunications perspective we have worked closely with. The first one is Telco forum, which consists of 21 suppliers, and that forum interactively with those suppliers tested 82 different telecommunication elements. And those elements were chosen as a result of them being representative across Northern America.

When you start looking from an overseas perspective and long distance calls completing, the other organization which we conducted testing with is known as ATIS, the Alliance for Telecommunications Industry Solutions. Those testing has been done and the results have, in fact, been successful.

Mr. LE NAEVE. In our case, most, if not all, the power we purchase comes from the organization, from the Western States Coordinating Council or those agencies that are members, and, as Mr. Hall says, we're now encouraged that Canada is on board. And speaking for SMUD, we believe they are at least as well off in being prepared as we are. And I'm even more encouraged after today because the bulk of the power we buy, we get it from PG&E. So I'm satisfied.

Mr. OSE. How about at the airport? I know we have—we have a single carrier coming into the airport from foreign—Canadian Air, can they fly into Sacramento airport?

Mr. FERGUSON. Personally, I'm not familiar with all the carriers out at the airport. I did want to mention one other public—quasi-public utility. Sacramento County and the Office Communication Information Technology operates Sacramento Regional Radio System, which supplies public safety radio services to all the agencies in the region. We operate a system that contains about 8,000 portable and mobile radios and supplies communication services to the sheriff, the police department, utilities, the fire districts. That system has been tested and is Y2K compliant.

Mr. OSE. Well, gentlemen, I want to say that I appreciate you coming down here. What I hear you saying is the systems are going to be ready, and I can tell you as a representative of a large agricultural area and numerous urban areas, you give me a great deal of comfort in that respect. I'm going to hold you accountable.

Mr. Chairman, anything else?

Mr. HORN. No, that's it. That was asked.

Mr. OSE. I got this covered. Let's go ahead and release this panel. Again, our appreciation and bring the third panel down.

So we need to have Kathleen Tschogl, Alan Rabkin, Guy Koppel and Holly Delaney.

I saw Kathleen walk out the back of the room. Better get in here, we're waiting on you.

Mr. Willemssen, you might want to just sit up here because you'll probably have to move back up here eventually.

As we have with other panels, I would like to swear you in as we do with every other congressional testimony, so if you'll rise.

Do you solemnly swear that the testimony you will give before this subcommittee will be the truth, the whole truth, and nothing but the truth?

Let the record show the witnesses answered in the affirmative. [Witnesses sworn.]

Mr. OSE. We're going to start with Kathleen Tschogl from Raley's. She's the manager of governmental and regulatory affairs with Raley's Supermarkets. Please go to the podium to present your testimony.

STATEMENTS OF KATHLEEN TSCHOGL, MANAGER, GOVERNMENTAL AND REGULATORY AFFAIRS, RALEY'S SUPERMARKETS; ALAN RABKIN, GENERAL COUNSEL, SENIOR VICE PRESIDENT, SIERRA WEST BANK, ON BEHALF OF THE CALIFORNIA BANKERS ASSOCIATION; GUY KOPPEL, CHIEF INFORMATION OFFICER, U.C. DAVIS MEDICAL CENTER; AND HOLLY DELANEY, YEAR 2000 PROGRAM, MERCY HEALTHCARE SACRAMENTO

Ms. TSCHOGL. I didn't bring any pictures because they say that a picture is worth 1,000 words. So I just brought 1,000 words. I hope that's OK.

Mr. OSE. We have a picture here.

Ms. TSCHOGL. OK. On behalf of Raley's Supermarkets, I'd like to thank you for the opportunity to speak before you today about the issue of Y2K and the food industry. With the year 2000 only a few months away, resolving this problem is an urgent necessity. It's been estimated that the average major food company will spend $27 million to become Y2K compliant, combining to an industry total of $1.8 billion. You will be relieved to know the Grocery Manufacturers of America reports that 95 percent of its members have already completed and tested their Y2K upgrades. The overwhelming amount of time and money invested leaves us confident that the food industry will be well prepared for the year 2000.

At Raley's we began upgrades in 1997 by analyzing and testing our current systems, including telecommunications, internal software, and point of sale hardware. These upgraded systems have been operating successfully since June 30th of this year. An area of great concern to our customers is the electronic funds transfer, the EFT network. Debit and credit card terminals at cash registers are run by computers, and many people fear they will be either unable to use their ATM cards or that inaccurate transactions will take place. To solve this problem, Raley's and other supermarkets have completed certifications with their EFT network providers on Y2K readiness.

Perhaps even more important than attending to one's own Y2K problems is making sure others are taking care of theirs. In an industry so heavily reliant upon a network of suppliers, manufacturers, shippers and retailers, it is essential that every link in the supply chain be strong enough to handle the new millennium. We're working closely with vendors and suppliers on their Y2K compliance efforts. We keep a list of all outside companies who may possibly affect our Y2K readiness and receive regular updates on their efforts.

The great amount of media hype surrounding Y2K have customers worried that food shortages will occur and that their supermarket's shelves will be empty. The food industry has been hard at work since 1997 to make sure that this does not happen.

We would like to remind the public that grocery stores are well accustomed to dealing with natural disasters, storms and holiday rushes. We are no strangers to providing goods and services during the harshest conditions. We are completely capable of ordering and receiving additional supplies as necessary. No change in supplies expected. We urge customers not to stockpile any more water or food than they would normally do in preparation for winter. The bulk of our concerns are not internal but related to outside government programs and regional utilities. These are areas beyond our control. We as an industry urge the government to provide support and oversight so that these crucial systems operate efficiently, allowing goods to be manufactured, transported, and supplied to the public.

Another possible Y2K concern is connected to the food assistance program. Many of our customers rely upon programs such as WIC and food stamps. These programs often rely upon electronic benefit transfers creating a possible Y2K problem. While they are not under the industry control, we have been working with the USDA to prepare these systems for the new millennium. We request the Government give the necessary attention to the programs in connection to the Y2K issue so that we may continue to serve the people who rely on them.

We take our responsibility to provide for the people seriously. We've been working to ensure that our customers' needs will be met. We have tested, retested, and reinforced our systems for the year 2000. Raley's plans to have a Y2K team on hand throughout the New Year weekend to handle any complications that may unexpectedly arise. We are more than prepared for the year 2000.

Thank you.

Mr. OSE. Thank you.

[The prepared statement of Ms. Tschogl follows:]

The Food Industry and Y2K

With the year 2000 only five months away, resolving the Y2K problem is no longer a distant goal, but an urgent necessity. Nearly every industry has been affected, and has scrambled to update computer systems to survive the change of the millennium. It is of paramount importance that the food and grocery industry is more than prepared, we must be flawless in providing for the public's needs through the millennium transition. The Grocery Manufacturers of America (GMA) estimate that the average food company will spend $27 million to update computer systems, combining to an industry total of $1.8 billion spent on Y2K readiness. The GMA's members also indicate that they have been addressing Y2K problems since as early as 1997, often working around the clock, testing, updating and re-testing. The overwhelming amount of time and money invested in planning for Y2K leaves us confident that the food industry will be well, if not perfectly, prepared for the year 2000.

Early recognition of the Y2K problem prompted the food industry to begin implementing solutions long before other industries. As a result, the GMA reports that 95% of its members have completed and tested their Y2K compliance updates, with the majority completed in May, 1999.

Raley's began the upgrades in 1997 by analyzing and testing our current systems including telecommunications, internal software and point of sale hardware. The majority of our efforts were focused on our software systems containing the two-digit date system. On January 1, 2000, many computers will read this date as January 1, 00, since computers only store the last two digits of the year. The fear is that the computer will not know what century this 00 belongs to and shut down as a result of the confusion. Raley's has implemented the popular "49/50 windowing technique", which solves the two digit date recognition problem by programming the computer to recognize all date fields between 0 and 49 as the century of 2000, and all date fields between 50 and 99 as the century 1900. In the cases where this technique has failed, computer software has been successfully altered to accept four digit date fields, instead. To insure smooth store service, Raley's has also introduced new, Y2K compliant point-of-sale hardware and has been operating successfully with the new system since June 30, 1999. Raley's has also completed certification with our Electronic Funds Transfer (EFT) network provider on Y2K readiness. This insures customers that all stores will be able to process credit and debit card transactions during the new year. Rigorous testing of "embedded systems" has been important as well. Assessing and testing all systems that are not managed under formal technology, such as elevators, alarm systems and energy management is an ongoing process. Systems which demonstrate a need for Y2K attention are added to the Year 2000 master plan for compliance upgrades.

Perhaps even more important than attending to one's own Y2K problems, is making sure that others are attending to theirs. In an industry so heavily reliant upon a network of suppliers, manufacturers, shippers and retailers, it is essential that every link on the supply chain be strong enough to handle the year 2000. The greatest potential danger lies not in a huge, industry wide computer crash, since this is highly unlikely, but in a small glitch in one supplier's program causing a ripple effect of problems and delayed service to all other companies. This is why an integral part of our Y2K readiness has included the testing of outside vendors and supplier's compliance. Because we in rely upon one another so extensively, we have been working closely with our suppliers to guarantee a Y2K glitch of theirs, will not impact or diminish our careful preparations. This is a complex and time consuming task. A great deal of information is transmitted between companies by electronic file transfer. A computer problem could disrupt this information and cause breaches in service to the customer. Since 1998, Raley's EDI and other file transfer systems have been Y2K compliant. Raley's keeps a list of all vendors and outside suppliers who may affect our Y2K readiness and coordinates Y2K upgrades for these companies, and/or receives regular notification of their internal compliance efforts. Similar "checks and balances" are happening throughout the food industry, assuring that the chain of supply will withstand any year 2000 problems.

A special amount of attention has been applied to the area of international commerce. Many consumers and companies are worried about the preparedness level of other countries. The food industry relies heavily upon international trade to stock the grocery aisles. Multinational corporations have expressed a desire to be Y2K ready, and for the most part we expect no disruption. In areas where some doubt of compliance remains, the food industry is working with these companies to become Y2K prepared. Most international companies will be adequately updated for the new year. In the event that problems do occur with non-compliant trade partners outside the United States, domestic suppliers and the U.S. offices of international companies will be able to supply the additional food needed to account for any international product loss.

Perhaps the greatest comfort to the public is knowing that the food industry, unlike many other industries, is accustomed to dealing with crisis situations and supply problems. Natural disasters, winter storms, and holiday rushes have made Raley's, and other companies alike, no stranger to providing service and supplies throughout the harshest of conditions. All grocery stores keep a stockpile of canned goods and non-perishable goods to prepare for the possibility of an emergency or unexpected shortage. Furthermore, most grocery stores have increased their inventory in preparation for specific Y2K related needs. Buyers for the markets have been instructed to treat the New Year as any other busy holiday season, and order for high volume sales. Raley's is completely capable of ordering and receiving additional supplies if needed - provided onsumers do not act unnecessarily rash in their purchases. No change in supply of oods is expected. All grocery and household items will be sufficiently stocked and vailable to consumers. The food industry is urging consumers not to stockpile any more water and food supplies than they normally would in preparation for winter. Media hype and the public's fears could cause an isolated, very temporary shortage of certain items, if customers buy inordinate amounts of goods.

In regards to electricity, heating and water in our stores, we expect no problem. The majority of these systems have already been updated for the year 2000. In testing and planning for potential failures, most of our efforts have been concentrated on more rural areas, where the utility companies may not be as well equipped to deal with Y2K. Raley's has been busy planning for these needs, with back up generators, batteries and complete testing of all store systems. Most store systems, such as energy management, lighting and refrigeration, do not use dating in their programs and will operate as usual in the new century.

The bulk of concerns for the food industry are not internal, but related to outside government programs. National telecommunications, water and power services are beyond our control. We, as an industry, urge the government's help in maintaining these critical systems so that foods may be transported, manufactured and supplied. We ask any system in question be replaced or updated to help us provide supplies and services to the nation. Another concern of ours is connected to the food assistance programs. Many of our customers depend upon assistance programs such as Women, Infant and Children (WIC) and Food Stamps. Many of these programs rely upon electronic benefit transfers, creating a possible Y2K problem. While they are not under industry control, the food industry has been working with the USDA to prepare these systems for the new millennium. It has been an established request of ours that the government address these concerns through testing, upgrading and assuring complete readiness of the food-assistance programs.

On the whole, the food industry has been attentive and thorough in its preparations. A great deal of planning, time, money and cooperation has made experts and trade associations such as the Food Marketing Institute and the Grocer's Manufacturers of America confident that the industry will be among the most prepared. U.S. Secretary of Agriculture Dan Glickman told the U.S. Senate Committee, "The state of readiness in the food industry is encouraging. It is most likely the effects from the year 2000 problem will be minor and localized by region or particular food products. Competition in the vast majority of communities across the country will insure that food remains available even if some companies experience Y2K related problems."

Raley's and the food industry take our responsibility to provide for the people very seriously. We have been working to assure the entire nation's needs will be met. It is a great challenge to ready an industry infrastructure as complex as the food and grocery, but larger obstacles such as storms, earthquakes and floods have been surmounted in the past. We are confident that the year 2000 will be no different.

Mr. OSE. Mr. Rabkin, general counsel, senior vice president of Sierra West Bank, testifying on behalf of the California Bankers Association.

Mr. RABKIN. Thank you very much. I appreciate the opportunity to be here today and to speak to you concerning the banks' readiness for Y2K.

My name is Alan Rabkin. I am the general counsel and senior vice president of a regional bank by the name of Sierra West Bank, which was recently acquired by Bank of the West.

Now we serve the eastern California and western Nevada markets, so I can speak to you on those issues, but I'm generally familiar with what banks are doing nationwide. I'm knowledgeable about the banks' security aspect of Y2K since I served on SCC panels to formulate rules concerning that issue. I've seen firsthand the operational lending and other aspects of the year 2000, and I hope I know what I'm talking about.

Well, I've got good news for you. I think this is the shining moment for banks in the United States. We have done our work. We have gotten down to business. We have made our equipment ready. We have ordered new equipment when it's not ready. We have fixed and tested, retested, created plans and educated the public and our customers. Together we have assessed risks, account risks, loan risks, facilities risks. We canceled staff vacations. We've generally taken our lumps on 1999 earnings. We basically have done what a responsible bank should do, but we're not completely done. We always have things to do, but we certainly are through the door of compliance and we will meet the dawn of the new millennium with completely updated, fully compliant Y2K systems.

I like to say in my public presentations that if Father Time needs cash at the new millennium, we will deliver it. So what does this mean? What can we expect? Are there going to be major problems in the Y2K systems for banks?

The answer is, I can't predict exactly what will happen, but I will tell you that I doubt it. Some of you have read about recent problems in Y2K areas dealing with banks. Just about a week ago I opened the papers and there was an article about a company by the name of Affiliated Computer Services, a small Texas-based ATM provider who seems to have some sort of Y2K failure in their software systems. But when you look into the problem, it wasn't Y2K related at all. Instead, it was simply a software upgrade failure. It was simply a lack of fully engineered upgrade. And that happens a lot these days.

Recently in the area I'm in, a local regional airline carrier introduced an upgrade not related to Y2K, and that upgrade did not take well, and their whole system went down, they backed up with their prior system, they made the fixes and they came back on line.

This is the reality of computing in the 1990's. So once you get beyond the potential for errors caused by new software introduction, I think you'll find that banking has very, very few Y2K problems left to it. In fact, I myself still have all my money—or most of my money in FDIC-insured institutions. I'm fully confident I won't lose one dollar. I'm fully confident I'll be able to withdraw as much or as little money as I need. I'm fully confident my cash needs will be met on a day-to-day basis. I do need money to get through the end of the year and probably the best New Year's celebration of the millennium. However, I don't think I need my life savings to do that.

What's more of a Y2K concern to me, however, is the misinformation that I see daily. You know Y2K is good theater, and I'm getting a little tired of it, especially when it comes to ads like those run by KIA Motors Corp. implying that banks are not Y2K compliant. Frankly, there's no proof for that. In fact, there's opposite proof. All the Federal banking agencies, the Securities and Exchange Commission, even Alan Greenspan have represented banks as the poster child of Y2K compliance. We are the good conduct citizens of Y2K. We got started very early.

So what's all this misinformation about? Well, the L.A. Times came out with a story about a week ago saying even though it's been shown that banks are 99 percent compliant, that 42 percent of the consumers still believe ATMs will not operate. And 38 percent fear checks will bounce, and 20 percent believe that Y2K will shut down the banks.

So we have to do a better job. We have to market our skills better in Y2K. We have to get the word out that banks are fully compliant, and if there are any glitches they will be dealt with. So we are going to be more proactive. We're going to market Y2K just like we market our bank products. I think you've seen that recently with banks such as Union Bank who have the "Y2K OK" campaign going statewide right now.

Every delivery system will be used to get the word out between now and the end of the year; statement stuffers, public speaking, these hearings. Everything so that we can get face to face with our customers. And we will ask the customers what they are not aware of, what they need more information on, and we will be good corporate citizens going into the end of the year.

So with that proactive attitude, we continue to win the race. We continue to be up front and we feel that Y2K if it's not a dud, will certainly be a dud as to banking. So I'm here to answer any questions you might have concerning the banking industry, but we have arrived. We may have to be at work on January 1st just to be sure; but if you see us a little tipsy on January 2nd of the new millennium it's because we're celebrating a very, very good performance by the banking industry.

Thank you.

Mr. OSE. Thank you, Mr. Rabkin.

Mr. Koppel, who is the chief information officer of U.C. Davis Medical Center is here to join us, also.

Mr. KOPPEL. Thank you and good morning. First, let me apologize, I have neither a picture nor a thousand words prepared. We had some communications mix-up and we just—last evening I found out I was selected to appear here this morning. I would like to address the Y2K issues in terms of UCD Med Center and the health system. The health system is the combination of the school of medicine and the medical center. We in the health systems began looking at Y2K issues back in 1995 and 1996 and we took advantage of opportunities with our electronic systems to begin modifying in-house development, and making sure we had tractional language for acquisition of new systems.

In 1997 the university office of the president started formalizing the process and brought all the university medical centers and campuses together and developed a reporting system in which we participate. In July 1998 the UC Health Systems in Sacramento developed a task force. I co-chair that task force, and we have representatives from all across the organization that represents major operations and functionality areas. We developed an action plan, which tests all the obvious processes: Inventory, assessment, renovation, all the things that are necessary for Y2K readiness.

The major areas of concern that we have are—because we're in the patient care business, of course, trying to be self-sufficient in case everything fails. So the areas that we've looked at are not only information systems, but our health and safety areas with fire alarms, water and power. And I'd just like to say in terms of water and power, we're very fortunate to have a brand new power plant that is driven by natural gas. It has a secondary backup system, diesel. Our third redundancy is SMUD, and our fourth redundancy is portable generators that will plug into each of our major buildings. As far as water goes, we're depending on the city, but we have two wells in place right now, the third one going into the infrastructure is being constructed. I don't think water and power will be an issue.

Most of the medical equipment that we have is another major issue. We've notified vendors. We inventoried all of our equipment. We have tested it and set aside funding for acquisition of new equipment as we realize in some cases the vendors will not be upgrading for Y2K compliancy. Most of the orders for the new equipment and replacement equipment have been submitted, and will be on hand well ahead of the Y2K time period.

As far as office automation and facilities go, we've taken all kinds of measures to make sure that our office automation has contingency and business continuity depending on those systems. We put into place a program whereby we can interrogate and mitigate any PC-related problems in terms of resetting clocks, replacing chips or parts in the PCs. We've also addressed the issues of contracts, making sure that all of our contracts with people we do data exchange have Y2K compliant statements. We've notified all of our vendors and have gotten responses back from vendors regarding supplies and availability of supplies.

As far as the actual Y2K orientation itself, we have been audited by the State Division of Audit and we came through fairly good. The audit report would say that there is one system that they looked at, that had a plan for testing, but at the time they looked at it, it wasn't tested due to the fact that we had to add some equipment. That system has now been tested and validated. Most all of our electronic systems have been modified, replaced, tested and validated. For those that are not completed will be completed, those well ahead of year 2000.

The plan that we have at the Med Center is that we're going into the year 2000 very optimistically, but we also are going to hedge our bets by having a full staffing of our disaster recovery center, and we're going to be having full staff of any major area of concerns.

Telecommunications, I'd like to talk to you about that for a minute. We're self-sufficient. We have our own switching system. We have a backup, Pac Bell. We utilize an 800 megahertz radio system which is connected for emergency purposes to the county of Sacramento, and we also have an emergency phone system that is hard wired throughout the medical center in case of failure of Pac Bell or in our own switching systems.

I think that kind of concludes what I'd like to say, and I'd be happy to answer any questions.

Mr. OSE. Thank you, Mr. Koppel. We're going to take questions at the end of all the testimony.

Finally, our last panelist is Holly Delaney, who is in charge of the year 2000 program with Mercy Healthcare Sacramento.

Ms. DELANEY. I'd like to thank you, Congressman Ose and Chairman Horn, for the opportunity to present here today Mercy Healthcare Sacramento's Y2K preparedness status. As you may or may not know, Mercy Healthcare Sacramento is a division of CHW, which is located down in San Francisco. They are a 48 Facility Healthcare System. We here in Mercy Healthcare Sacramento have seven hospitals, including skilled nursing facilities, home health organizations and clinic locations known as Med Clinic in the area.

We began our year 2000 program in 1997 by developing an impact analysis. At the time the study identified 21 application system upgrade projects at a total of $2 million. In addition to that, we developed a Project Management Office at the corporate level that addresses all Y2K processes; including testing methodologies, standards for application systems, biomedical devices, facility equipment, computer hardware and network electronics. The PMO has tested all of our biomedical devices throughout our 48 facilities, our clinic locations and home health locations, et cetera, facilities equipment, which means elevators, alarm systems, fire suppression systems, et cetera, application systems and PC hardware, network and telecom.

We, like most organizations, have utilized the seven-phase Y2K compliance approach, which I'm sure you've heard a little bit about today: Inventory, assessment, planning, upgrade, testing, remediation and contingency planning. With limited staff resources and a set time for completion for Y2K, Mercy instituted a Y2K project prioritization process to ensure our patient critical Y2K systems were addressed first, so that we could continue to provide excellent quality patient care as we have for the last 100 years.

Our current Y2K status, interesting how quickly these numbers grow after you continue to investigate, has gone up to an estimate of $15 million effort, with 26,000 staff hours to make our medical equipment and support systems Y2K compliant.

Mercy has since identified a total 108 application systems upgrade projects, 63 of which we consider patient critical systems. And out of a total of 12,829 biomedical devices identified only 344, which is about 3 percent, failed our Y2K testing and either required replacements or upgrade. So that's pretty good news for the community at large that patients pretty much can rely on biomedical devices. That would be things like IV pumps, EKG machines, defibrillators, et cetera. Only 3 percent of these were determined to be noncompliant through our testing efforts, and we are in the process of remediating all of those.

Our current status, 84 percent of our patient critical applications systems are currently Y2K compliant. They have been tested and upgraded. By August 31st we believe 97 percent of our patient critical application systems will be Y2K compliant. All PC network telecom equipment will be Y2K compliant by the end of August, and all biomedical devices and facility's equipment will be Y2K compliant by September. All contingency plans are currently complete. They have been distributed to all the departments in our organization and we'll be undergoing a quality review process at—I believe it's next week, to test those plans out and our staff's ability to follow and understand those plans.

The various issues that we found in addressing our Y2K problem are that hardware and software vendors have continually changed their Y2K compliance status, causing us to reevaluate our cost, staff resources, and project completion dates. Many of our small software vendors are charging excessive fees and are slowing down our upgrade process for becoming Y2K compliant. These are the one-man, two-man owned shops with PC-based software that are basically holding us hostage at times because they just don't have the wherewithal to complete all the upgrades.

Third party software providers, we call them trading partners or EDI trading partners, both the data people and the vendors that we get supplies from at times cannot be tested or upgraded by Mercy. This includes some of our electronic claims remittance providers. We do have some risk in that area. However, we've mitigated this risk through contingency planning and basically we have manual processes in place by which we can continue to submit claims in a manual method.

In addition, small isolated PC-based systems were difficult to inventory. And I'm sure everybody who is dealing with the Y2K effort has identified that. Thus, they're being identified as we complete our PC upgrades. This provides very little time for us to remediate. However, these are not patient critical systems, and they are mostly business systems used for efficiency, not the core critical business system processes.

We're concentrating on contingency planning for these systems and basically people will have to do these efforts manually. Thank you.

Mr. OSE. Thank you, Ms. Delaney.

If you followed our panel list, you'll see that panel one is largely State and local government with a municipality. Panel two is largely utilities; and panel three is largely food, money, and health care kind of thing. So there is some sense or some method to our madness.

If I may, Mr. Chairman, I'm going to proceed with my questions; and you can wrap up, and we'll do the paperwork, if you will, kind of thing.

Ms. Tschogl, one of the questions I have is it—and it relates to Mr. Rabkin, also. The electronic funds transfer mechanism that many of your customers use, I want to make sure people understand that that's going to work when they come in at the end of the year, that the transactions are going to be accurate, that the system is going to be available. As I understood your testimony, that was the case that you have spent considerable effort making sure in conjunction with your partners, your business partners, that that will be available for folks?

Ms. TSCHOGL. Our information services people have confirmed to me that they are absolutely certain that the electronic funds transfer mechanism will be working. You can probably talk more about the electronics.

Mr. OSE. Turn that mic.

Ms. TSCHOGL. Turn this?

Mr. OSE. There you go. Much better.

Mr. RABKIN. Mr. Chairman, fortunately, the regulators—banking regulators have not stopped at banks. They've gone out to the vendors of banks and have examined vendors of banks on both mandatory and cooperative basis. On each of the primary Federal regulators both the Fed at fed.gov or fdic.gov or occ.gov you'll see listings of critical vendors like First Data or FDR, who are the primary drivers of what we call ACH or bank-card type transactions, and they've gone out and rather than make each bank test their driver of these systems, they've gone out and tested them with all the resources of the Government, which is very helpful. And, also, some enlarged banks have double-checked those findings and have checked the primary vendors as well and those noncompliant vendors are shown with their noncompliance status; but most, I would say, generally all, of the primary drivers of these very critical ACH wire transfer-type scenarios have been checked by the banking regulators.

Mr. OSE. ACH is Automated Clearing House?

Mr. RABKIN. Clearing House, that's correct. So this is not just one particular bank telling you that this will happen appropriately. It's the banking regulators telling us all that it will happen appropriately, and that's why I have comfort in it.

Mr. OSE. So folks are engaged in electronic commerce whether they be on vacation or down at the grocery store or out in the rural areas buying feed or fertilizer and they wish to do electronic commerce. It seems as if the system is prepared whether it be at Raley's or at Henry Miller's Implement Dealer up in Yuba City or whomever. The system appears to be prepared for that ability to be achieved.

Mr. RABKIN. That's correct. From what I've heard today, and prior testimony, we'll have power. We'll have phones. We'll have the banking and driver systems. Those are the critical elements to transacting any debit/credit transaction in any bank or merchant situation. So we have all the critical core elements to transact those transactions.

Mr. OSE. So the financial system will be available. Let me explore, if I might, a little bit one issue that comes up regularly that we're all very attuned to whether we live in cities or in rural areas is food quality. And I know Raley's has an ongoing extensive program for food quality.

Are there—is there any indication that there will be anything but a consistent high level of quality of product in the grocery stores by virtue of anything related to the Y2K problem?

Ms. TSCHOGL. Absolutely not. There will be no change whatsoever; and as I mentioned earlier, we have dealt with power outages before, and in the event in a rural community or outlying area there really is a power outage, we've done this before and we have backup generators that will operate efficiently. Our refrigeration units are going to operate efficiently, just like they have every other time that we've had a little glitch in the system. This is not going to be any different.

Mr. HORN. If I might just ask a question here. How about bottled water, will a lot of people do you think——

Ms. TSCHOGL. We predict that there will be people buying a lot more bottled water than they normally would, but I don't predict they are going to be buying that bottled water a week before the new year. I think they are probably going to start gearing up for it throughout. It's not necessary, but I do think that people will be doing this. There will probably be a run on plastic—empty plastic bottles for putting their own water in, but it's not going to be a crisis situation at the supermarket.

Every major supermarket has been preparing for this for years, and it's not what turned out to be at one point was a computer problem has escalated into another problem. That's all of our own making in our imaginations here about what's going to happen with food shortages.

Mr. OSE. I hear you saying——

Ms. TSCHOGL. And batteries. There will be no price gouging either, I might add. I don't know if you were going to ask that question, but that is another concern that some people have, that batteries are going to go for four dollars each when it gets into a crisis situation. I think you may have some of that. In some areas it may happen, but it won't happen in any of the major supermarkets across the country. I can speak for my colleagues in other supermarket chains that I won't mention.

Mr. OSE. If I may follow on, Mr. Koppel and Ms. Delaney, I know that Ms. Delaney's organization just opened a state-of-the-art trauma center out near my home town, if you will, actually it's in Carmichael. We're going to claim it's in Citrus Heights anyway. I want to make sure, one thing I heard Ms. Delaney talk about was the compliance levels in equipment, but I didn't hear Mr. Koppel speak about that. I wanted to come back to that, particularly as it relates to embedded chips and equipment that's been held for a couple, 3 years. You were very clear that you're down to about a 3 percent noncompliance rate.

Ms. DELANEY. That's what we started with.

Mr. OSE. You're even below that now?

Ms. DELANEY. Correct. We'll be 100 percent compliant with our biomedical devices by September.

Mr. OSE. Is that going to be the case also at the Med Center?

Mr. KOPPEL. We've identified—I thought I spoke to that issue, but I probably brushed over it quickly. We took an inventory and made a complete assessment of all of our medical equipment and to date we have purchased approximately $270,000 worth of equipment that we think needs to be replaced such as defibrillators, heart fusion pumps and small items. We expect there will be a few more. I can't tell you what the percentage is, but it's a fairly low percentage in comparison to the overall amount of investments that we made. The only medical equipment that is outstanding in terms of actual proof testing is some of our larger equipment like our MRIs, some CTs, cardiac catherization units, and the reason those are untested is because the vendors have notified all the users not to test these systems in the field. They are being tested at the factories and wherever else they have their testing sites. The reason being is some of these systems are so complex, if you set the time ahead, there's no going back on it. So it will just mess up the operating system; but except for that, we have plans to replace and we have the funding to replace all equipment that is not Y2K compliant, and it will be in before Y2K.

Mr. OSE. Ms. Delaney—I appreciate that. Ms. Delaney, you brought up something I thought was particularly farsighted, and that was the claims submittal process for people who are enrolled in HMOs or who are on Medicare or Medicaid or Medi-Cal. It's clear that Mercy in particular has given some thought to making sure that claim process doesn't bog down and become a nightmare either. Can you just kind of go over that for us briefly, please.

Ms. DELANEY. The biggest difficulty that we have found is in third parties claims administrators. Generally they have software that they've developed in-house and one in particular we're having difficulty getting upgraded.

Mr. OSE. Turn that mic around a hundred and eighty degrees. There you go. Nope, that's wrong.

Ms. DELANEY. I'll just talk closer. How's that?

So that is one of the difficulties we are finding. However, that won't prevent the provision of patient care. That just prevents us from getting our money for the provision of patients' care. So although we're concerned about it from an organizational standpoint, our patients should not be concerned at all. As I said, we do have provisions to submit those claims manually, and we are working as a corporation with some of those organizations to provide our clout to get those systems rectified and Y2K compliant. But that is an issue the third-party payors are not always compliant.

Mr. OSE. We have a very large organization in the U.S. Government called the Health Care Financing Agency [HCFA] in particular has had some difficulty just making sure that they are going to be compliant. Are you anticipating any difficulty there? And when you're finished, Mr. Willemssen, I'd appreciate any input you might have on this particular issue, too, with respect to Medicare claims and the like.

Ms. DELANEY. No. I read the reports on HCFA and I'm pretty sure—I know—they actually in the past have instituted—for example, when they've changed large computer systems, they've instituted a continued payment system, so I'm pretty sure that if anything should happen with the payment system, what they will probably do is just continue the average payments to the healthcare systems. So we're pretty confident that that won't be a financial risk to us.

Mr. WILLEMSSEN. HCFA and Medicare represent one of the highest risk Federal programs that remains. The administrator has made a lot of excellent progress, but because they got such a late start and they have such a widespread intricate heavily computerized set of systems, they still have a long ways to go and limited time to do it. They are still overlapping remediation and testing activities that are occurring over the next few months. So there is still reason for concern.

Reason for optimism is similar to what she pointed out. They have done a lot of good efforts in the contingency planning area, so that in the event there are disruptions, they will be prepared with backup plans. Those backup plans still need some further refinement and testing, however. So overall there's still definite room for concern on HCFA and Medicare. They are aware of it. They are working as aggressively as possible on it.

If I also might point out, Congressman, in relation to comments you made earlier on biomedical equipment, I thought it useful to point out, I don't believe the witnesses had mentioned that there is a FDA data base on biomedical equipment that includes Internet links to over 400 manufacturers, and it indicates what those manufacturers say about their items. We've looked at that and there are over 35,000 products identified by those manufacturers, and about 4,500 of them are considered noncompliant. It may be—if the witnesses here haven't already done so, it may be worth their while to compare their efforts against what's reflected in those websites so it can match up any anomalies.

Mr. HORN. On that point, Mr. Chairman, you were with us at the Cleveland hearing, I believe, and the very excellent representative from the Cleveland clinic talked about how they have this site where all the emergency room equipment could be checked against that, and the UC Davis submission is very impressive on how you people have been at this for a long time and well organized. I'm just curious, have you used the same site as the Cleveland clinic and a lot of them are using?

Mr. KOPPEL. I'm not aware that we have. I know that we're working in conjunction with the purchasing department I know they have went out and interrogated these sites, and I'm sure they are working very close with our technical engineering department along these lines. I personally am not aware of that.

Ms. DELANEY. I have a quick comment about biomedical devices. CHW, when they began testing or when they chose to look at biomedical devices, found it was very difficult even from the manufacturer to determine which biomedical devices were Y2K compliant, because often the serial numbers didn't even reflect what embedded chips, et cetera, were in each device. So that's why we chose to go ahead and test all of our devices, and that is about 50 percent of the healthcare providers chose testing versus reviewing the data bases and the various information out there. We did choose to test because we started this early on, and we're very confident that we have the accurate information about Y2K because of that test.

Mr. OSE. Mr. Chairman.

Mr. HORN. I don't have any further questions. I think the panel has been excellent. I don't know if Mr. Willemssen has anything.

Mr. WILLEMSSEN. Nothing else to add, Mr. Chairman.

Mr. HORN. Thank you all. You were all impressive. You're right about the banks. We had them in our first hearing and the Clearing House and Mr. Greenspan and others have been doing a great job in making sure they comply, and the banks have done a great job.

Mr. RABKIN. Maybe we should be giving away bottled water rather than toasters.

Mr. HORN. How about plates in the Depression.

Mr. OSE. Lower interest rates.

Thank you all for participating.

Mr. HORN. We have thanks to the staff here. And our staff director for the Subcommittee on Government Management, Information, and Technology is J. Russell George, and he's the chief counsel for the subcommittee. And on my right—your left—is Bonnie Heald, the professional staff member responsible for this hearing and the director of communications for the subcommittee. And the gentleman who was alert and moving those microphones around was Grant Newman, our clerk. And we had a lot of help from Mr. Ose's staff. And we want to thank Dan Scopek and Donna Willborn with Metro Cable, production director, and we also had from Mr. Ose's staff, Tory—you pronounce it——

Mr. OSE. Tovey Giezentanner.

Mr. HORN. Tovey Giezentanner and Peter DeMarco. And our court reporter is Maria Esquivel-Parkinson, and we thank you very much for sticking with us. It's tough sometimes when you can't get a rest or anything else.

With that, if there are no further comments, I thank you for all you've done for this subcommittee.

Mr. OSE. I do have a closing remark, Mr. Chairman. Under your guidance we have been able to bring together here this morning government at all levels to talk about the challenges we face. We've been able to bring the critical utility providers together to talk about their level of preparedness. In my opinion, we've brought together the most critical elements of private industry, that being banking, food and delivery, if you will, and healthcare to talk about their relative levels, and this would not have happened without your interest and participation and those of us in Sacramento who will benefit from this. On their behalf I say thank you for taking the time to come.

Mr. HORN. Well, I thank you because I tell you, we've been through a lot of these, Mr. Ose and I and the staff, and just by chance and lot of hard work has been a really broad-based operation here, and I've been very pleased with the quality of testimony, both your oral testimony, your response to questions, as well as your written testimony which automatically goes in the record the minute the chairman recognizes you.

We're sorry we have to cut it down sometimes to 5 minutes, but we want to get to the questioning, and that's where we learn the most, we think, because we've already read your documents and we thank you all for coming and the panels before you.

And with that, we're going to recess this hearing to tomorrow in the Silicon Valley in San Jose. We will have the last hearing in northern California, and then we're going on to the State of Washington next week for year 2000 testimony with the help of the Discovery Institute, which is a major foundation in Seattle. So with that, if there's no further comments, this is recessed to San Jose tomorrow.

[Whereupon, the subcommittee was recessed.]

THE YEAR 2000 COMPUTER PROBLEM: LESSONS LEARNED FROM STATE AND LOCAL EXPERIENCES

SATURDAY, AUGUST 14, 1999

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY,
COMMITTEE ON GOVERNMENT REFORM,
San Jose, CA.

The subcommittee met, pursuant to notice, at 10 a.m., in the San Jose City Hall, City Council Chambers, North First Street, San Jose, CA, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representative Horn.

Staff present: J. Russell George, staff director and chief counsel; Patricia Jones, American Political Science Association congressional fellow; Bonnie Heald, communications director; Chip Ahlswede, clerk; Casey Beyer, chief of staff, Congressman Tom Campbell's district office staff.

Mr. HORN. This hearing of the House Subcommittee on Government Management, Information, and Technology will come to order. I'd like to welcome the residents of Silicon Valley, the San Jose Region for joining us today for the subcommittee's 11th field hearing on the year 2000 technology challenge.

The year 2000 computer problem affects nearly every aspect of operations in the government and the private sector. In Social Security and Medicare to local telephone service, electrical power and home personal computers, the year 2000 computer bug has certainly been a large management and technology challenge for all of us. No single organization, city, State or even country can solve the year 2000 problem alone, nor can they guarantee their computers will work until the organizations and agencies that exchange data with them are also compliant.

The year 2000 problem was created in the mid-1960's when programmers seeking to conserve limited computer storage capacity began designating the year in two digits rather than four. In other words, if you had 1967, they saved memory on 19 and put in 67, and that was pretty soon practice, and you had two-digit years. Now they knew there would be a problem when there was a year 2000 because it would register 00 and a computer probably wouldn't know whether it was 1900 or 2000 or whatever it was, and those systems might malfunction, corrupt data or shut down completely. But they were optimists. They're Americans. They said, "Technology will solve this." The fact is technology hasn't solved it. There's no silver bullet. It's a serious situation.

Our first hearing was held in April 1996, and we had the clearing house, the banks, a number of key parts of our society, and they have been working steadily to make sure that those basic economic indicators and processes in our society work. But our focus as the subcommittee has been on the executive branch of the Government of the United States, and we found them ill prepared. And it took them about 2 more years despite our prodding to get prepared, and they finally appointed an individual to give full-time efforts to it, and he's done an excellent job.

Mr. Koskinen is an assistant to the President and heads the Year 2000 Conversion Council, and we have had the pleasure of working with them. And our report cards you see out there on the desk are one of the prods we use to get them to face up to these matters, and slowly this is happening. We're optimistic. We think it will all be done prior to January 1, 2000. Current estimates show that the Federal Government will spend nearly $9 billion to fix its computer system in this fiscal year which ends September 30th. It might well go into another billion if there's the sort of panic mode, shall we say. If that's what we worried about in the beginning, let's have careful management, good organization and work systematically to achieve the goals, and they're finally getting that there. So as I said, I have faith that this will work. I have often said the figure will reach $10 billion, and it might.

Recently, the President's Office of Management and Budget identified 43 essential Federal programs such as Social Security, Medicare, and the Nation's air traffic control system. Each day these programs provide critical services to millions of Americans. Of those 43 programs, 10 are federally funded, State-run programs including Medicaid, food stamps, unemployment insurance and child support enforcement. Based on the data we received in May, all of these State-run programs were not scheduled to be ready for the year 2000 until December, leaving little, if any, time to fix unforeseen problems.

Data exchanges and interdependencies exist in all levels of government and throughout the private sector. A single failure in the chain of information could have very severe repercussions. For example, Social Security Administration maintains a data base of Social Security payment information for eligible citizens. One data base has about 50 million citizens registered in it and another 43. When these payments are due, the Social Security Administration sends that information to the Department of the Treasury's financial management service where the check is issued and either electronically deposited into the personal bank account of the client, or it's delivered by the U.S. Postal Service. Each of these agencies has its own network of computers. If even one of them fails, the entire system breaks down, and the check will not be delivered.

Indeed, many of the Federal executive branch agencies and Cabinet departments have said, "Well, our contingency plan is the U.S. Postal Service." When we saw that, we decided to hold a hearing with the U.S. Postal Service, and it turned out they had no contingency plan for themselves. So we're not sure about the various agencies on their fallback. But it will be slow. Fortunately, the Social Security Administration has been working on the problem for 10 years, and they're in good shape. And the only other one at this point 'til our next report is what we called in the old days the weather service. They're right on target. If there were still a few farms in the Santa Clara Valley, those farmers would be very happy. They could get all the weather news they want as they drive their tractors through the furrows and orchards of Santa Clara County, but they're hard to find anymore.

But even well-prepared computers won't work without power. One of the most essential questions involving the year 2000 challenge, and we'll have some testimony on this before us today, will the lights stay on? Without electricity our modern society would be relegated back to the proverbial stone age, and that would have a major effect on our economy. We remember the General Motors strike in Michigan? That would be a drop in the bucket compared to power outages, assembly lines stopping, hundreds of suppliers that make up some major products such as airplanes for my own constituency where Boeing and the former Douglas operations, suppliers come from all over America. So blackouts, inadvertent or vertent, I guess, they can cause real economic damage.

Our Nation has made great strides in the advancement of information technology to which we owe the credit to many corporate residents of Silicon Valley. We're extremely fortunate today to have as witnesses representatives from high technology companies that develop hardware, software, microchips and processors that enable our computer systems to function on a daily basis. We're very interested to hear how these companies have approached the year 2000 technology challenge and their experiences in dealing with this issue as we approach the new millennium.

No one can predict what might or might not happen once the clock ticks past midnight this New Year's Eve. The only certainty is that this January 1st deadline cannot be extended. So I welcome today's panel of witnesses.

[The prepared statement of Hon. Stephen Horn follows:]

ONE HUNDRED SIXTH CONGRESS

Congreſs of the United States

Houſe of Repreſentatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY	(202) 225–5074
MINORITY	(202) 225–5051
TTY	(202) 225–6852

"Oversight of the Year 2000 Problem: Lessons to Be Learned from State and Local Experiences"
Opening Statement of Chairman Stephen Horn (R-CA)
Subcommittee on Government Management, Information, and Technology
August 14, 1999
San Jose, California

This hearing of the House Subcommittee on Government Management, Information, and Technology, will come to order. I would like to welcome the residents of the San Jose region for joining us today for the subcommittee's eleventh field hearing on the Year 2000 technology challenge.

The Year 2000 computer problem affects nearly every aspect of operations in the government and the private sector. From Social Security and Medicare to local telephone service, electric power and home personal computers, the Year 2000 computer bug has certainly been a large management and technological challenge for all of us. No single organization, city, State or even country can solve the Year 2000 problem alone. Nor can they guarantee their computers will work until the organizations and agencies that exchange data with them are also compliant.

The Year 2000 problem was created in the mid-1960s when programmers, seeking to conserve limited computer storage capacity, began designating the year in two digits rather than four. The year 1967, for example, was shortened to '67.' The concern as we approach the new millennium is that computers will misinterpret the last two zeroes in the year 2000 as 1900, causing these systems to malfunction, corrupt data, or shutdown completely.

More than three years ago, our subcommittee held the first Congressional hearing on the Year 2000 problem. Since that time, we have held almost 30 hearings and issued 8 "report cards" monitoring the Year 2000 status of the 24 largest agencies in the executive branch of the Federal Government.

Current estimates show that the Federal Government will spend nearly 9 billion dollars to fix its computer systems. I have often said that figure will easily reach 10 billion dollars.

Recently, the President's Office of Management and Budget identified 43 essential Federal programs such as Social Security, Medicare, and the nation's Air Traffic Control system. Each day, these programs provide critical services to millions of Americans. Of these 43 programs, 10 are Federally funded, State run programs including Medicaid, Food Stamps, Unemployment Insurance, and Child Support Enforcement. Based on data we received in May, all of these State run programs were not scheduled to be ready for the Year 2000 until December, leaving little, if any, time to fix unforeseen problems.

Data exchanges and interdependencies exist at all levels of government and throughout the private sector. A single failure in the chain of information could have severe repercussions.

For example, the Social Security Administration maintains a database of Social Security payment information for eligible citizens. When these payments are due, the Social Security Administration sends that information to the Department of the Treasury's Financial Management Service where the check is issued and then either electronically deposited into a personal bank account or it is delivered by the United States Postal Service. Each of these agencies has its own network of computers. If even one of them fails, the entire system breaks down and the check will not be delivered.

Fortunately, the Social Security Administration has been working on this problem for 10 years and is in good shape.

But, even well-prepared computers won't work without power. One of the most essential questions involving the Year 2000 challenge is: "Will the lights stay on?" Without electricity, our modern society would be relegated back to the proverbial "Stone Age."

Our nation has made great strides in the advancement of information technology to which we owe the credit to many corporate residents of Silicon Valley. We are extremely fortunate today to have as witnesses, representatives from high technology companies that develop hardware, software, microchips and processors that enable our computer systems to function on a daily basis. We are very interested to hear how these companies have approached the Year 2000 technology challenge and their experiences in dealing with this issue as we approach the new millennium.

No one can predict what might, or might not, happen once the clock ticks past midnight this New Year's Eve. The only certainty is that this January 1st deadline cannot be extended.

I welcome today's witnesses and look forward to their testimony.

Mr. HORN. We will have two panels here and panel three after that.

And then the first one, I'd like to call those witnesses forward: Joel Willemssen, the Director of the Civil Agencies Information Systems of the U.S. General Accounting Office; Mark Burton, the Y2K project manager for the city of San Jose; Dana Drysdale, vice president, information systems, San Jose Water Co.; Ronald E. Garratt, assistant city manager, city of Santa Clara; Christiane Hayashi, the year 2000 communications manager for the city of San Francisco. If you will come forward, this is an investigating committee of the House, so we have the following process: We would ask you to stand, raise your right hands to affirm the oath to the truth of the testimony, and then I'll make some other requirements.

[Witnesses affirmed.]

Mr. HORN. The clerk will note that all five witnesses have affirmed the oath. As we introduce each one of you, your full statement is automatically put in the record, and these records get very thick as you can imagine, but you have some excellent information in the full statement. We would like you to summarize, if you could, to 5 minutes if you need a few more, OK. But if you could do it in five, that leaves time for a dialog between you and us, and between yourselves, and I think that is all very fruitful often, if we get that done.

So let us start, then, with the first witness we have, and he follows us around America, precedes us, and that is Mr. Willemssen, the Director of the Civil Agencies Information Systems for the General Accounting Office. That is an arm of the legislative branch since 1921, and they have given us outstanding service in terms of looking at this very tightly, both on the economics, on the accounting and on the programmatic arrangements. They put out, with every new Congress, a high-risk profile on the various agencies of the government, and we use that as a model to examine what the executive branch is doing. So Mr. Willemssen, it's all yours.

STATEMENTS OF JOEL WILLEMSSEN, DIRECTOR, CIVIL AGENCIES INFORMATION SYSTEMS, U.S. GENERAL ACCOUNTING OFFICE; MARK BURTON, Y2K PROJECT MANAGER, CITY OF SAN JOSE; DANA DRYSDALE, VICE PRESIDENT, INFORMATION SYSTEMS, SAN JOSE WATER CO.; RONALD E. GARRATT, ASSISTANT CITY MANAGER, CITY OF SANTA CLARA; AND CHRISTIANE HAYASHI, YEAR 2000 COMMUNICATIONS MANAGER, CITY OF SAN FRANCISCO

Mr. WILLEMSSEN. Thank you, Mr. Chairman. As requested, I'll briefly summarize our statement on the Y2K readiness of the Federal Government, State and local government and key economic sectors.

Regarding the Federal Government, reports indicate continued progress in fixing, testing and implementing mission-critical systems. Nevertheless, numerous critical systems must still be made compliant, and must undergo independent verification and validation. The most recent agency quarterly Y2K reports due to OMB yesterday should provide further information on agency progress.

Our own reviews of selected agencies have shown uneven progress and remaining risks in addressing Y2K, and therefore point to the importance of business continuity and contingency planning. Even for those agencies that have clearly been Federal leaders such as the Social Security Administration, some work still remains to ensure full readiness. If we look beyond individual agencies and systems, the Federal Government's future actions will need to be increasingly focused on making sure that its high priority programs are fully compliant. In line with this, OMB has identified 43 high impact programs such as Medicare and food safety.

Available information on the Y2K readiness of State and local governments indicates that much work remains. For example, according to recently reported information on States, about eight States had completed implementing less than 75 percent of their mission-critical systems. Further, while all States responding said that they were engaged in contingency planning, 14 reported the deadlines for this as October or later. State audit organizations, including the California State Auditor, have also identified significant Y2K concerns in areas such as testing embedded chips and contingency planning.

Another area of risk is represented by Federal human services programs administered by States, programs such as Medicaid, food stamps, unemployment insurance and child support enforcement. OMB recorded data on the systems supporting these programs showed that numerous States are not planning to be ready until close to the end of the year, and further, this is based on data that have not been independently verified.

Recent reports have also highlighted Y2K issues at the local government level. For example, in July we reported on the Y2K status of the 21 largest U.S. cities. On average these cities were reporting completing work on about 45 percent of their key services.

Y2K also remains a challenge for the public infrastructure and key economic sectors. Among the areas most at risk are health care and education. For health care, we've testified on numerous occasions on the risks facing Medicare, Medicaid and biomedical equipment. In addition, last month we reported that while many surveys have been completed on the Y2K readiness of health care providers, none of the 11 surveys we reviewed provided sufficient information to assess the true status of these providers.

For education, last week's report of the President's Y2K Conversion Council indicates that this continues to be an area of concern. For example, according to that report, many school districts could have dysfunctional information systems because less than one-third of institutions were reporting that their systems were compliant.

That completes the summary of my statement, and after the panel is done, I'll be pleased to address any questions. Thank you.

Mr. HORN. Thank you very much for that very helpful and thoughtful statement.

[The prepared statement of Mr. Willemssen follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10:00 a.m. PDT
Saturday,
August 14, 1999

YEAR 2000 COMPUTING CHALLENGE

Important Progress Made, But Much Work Remains to Avoid Disruption of Critical Services

Statement of Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division

GAO
Accountability * Integrity * Reliability

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting us to participate in today's hearing on the Year 2000 problem. According to the report of the President's Commission on Critical Infrastructure Protection, the United States--with close to half of all computer capacity and 60 percent of Internet assets--is the world's most advanced and most dependent user of information technology.[1] Should these systems--which perform functions and services critical to our nation--suffer problems, it could create widespread disruption. Accordingly, the upcoming change of century is a sweeping and urgent challenge for public- and private-sector organizations alike.

Because of its urgent nature and the potentially devastating impact it could have on critical government operations, in February 1997 we designated the Year 2000 problem a high-risk area for the federal government.[2] Since that time, we have issued over 130 reports and testimony statements detailing specific findings and numerous recommendations related to the Year 2000 readiness of a wide range of federal agencies.[3] We have also issued guidance to help organizations successfully address the issue.[4]

Today I will highlight the Year 2000 risks facing the nation; discuss the federal government's progress and challenges that remain in correcting its systems; identify state and local government Year 2000 issues; and provide an overview of available information on the readiness of key public infrastructure and economic sectors.

[1] Critical Foundations: Protecting America's Infrastructures (President's Commission on Critical Infrastructure Protection, October 1997).

[2] High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

[3] A list of these publications is included as an attachment to this statement. These publications can be obtained through GAO's World Wide Web page at *www.gao.gov/y2kr.htm.*

[4] Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, issued as an exposure draft in February 1997 and in final form in September 1997), which addresses the key tasks needed to complete each phase of a Year 2000 program (awareness, assessment, renovation, validation, and implementation); Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, issued as an exposure draft in March 1998 and in final form in August 1998), which describes the tasks needed to ensure the continuity of agency operations; and Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, issued as an exposure draft in June 1998 and in final form in November 1998), which discusses the need to plan and conduct Year 2000 tests in a structured and disciplined fashion.

THE PUBLIC FACES RISK OF YEAR 2000 DISRUPTIONS

The public faces the risk that critical services provided by the government and the private sector could be severely disrupted by the Year 2000 computing problem. Financial transactions could be delayed, flights grounded, power lost, and national defense affected. Moreover, America's infrastructures are a complex array of public and private enterprises with many interdependencies at all levels. These many interdependencies among governments and within key economic sectors could cause a single failure to have adverse repercussions in other sectors. Key sectors that could be seriously affected if their systems are not Year 2000 compliant include information and telecommunications; banking and finance; health, safety, and emergency services; transportation; power and water; and manufacturing and small business.

The following are examples of some of the major disruptions the public and private sectors could experience if the Year 2000 problem is not corrected.

- With respect to aviation, there could be grounded or delayed flights, degraded safety, customer inconvenience, and increased airline costs.[5]

- Aircraft and other military equipment could be grounded because the computer systems used to schedule maintenance and track supplies may not work. Further, the Department of Defense could incur shortages of vital items needed to sustain military operations and readiness.[6]

- Medical devices and scientific laboratory equipment may experience problems beginning January 1, 2000, if their software applications or embedded chips use two-digit fields to represent the year.

Recognizing the seriousness of the Year 2000 problem, on February 4, 1998, the President signed an executive order that established the President's Council on Year 2000 Conversion, chaired by an Assistant to the President and consisting of one representative from each of the executive departments and from other federal agencies as may be determined by the Chair. The Chair of the Council was tasked with the following Year 2000 roles: (1) overseeing the activities of agencies; (2) acting as chief spokesperson in national and international forums; (3) providing policy coordination of executive branch activities with state, local, and tribal governments; and (4) promoting appropriate federal roles with respect to private-sector activities.

[5] FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998) and Year 2000 Computing Crisis: FAA Is Making Progress But Important Challenges Remain (GAO/T-AIMD/RCED-99-118, March 15, 1999).

[6] Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998).

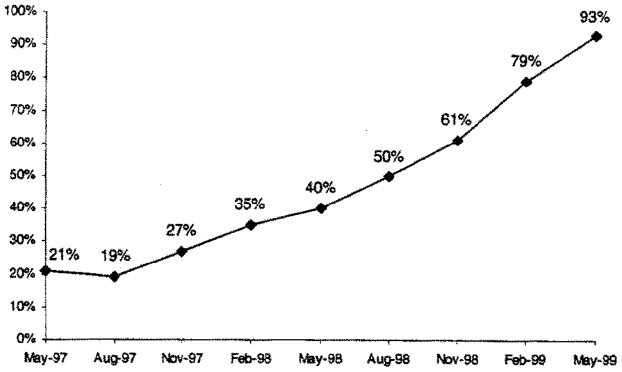
IMPROVEMENTS MADE BUT MUCH WORK REMAINS

Addressing the Year 2000 problem is a tremendous challenge for the federal government. Many of the federal government's computer systems were originally designed and developed 20 to 25 years ago, are poorly documented, and use a wide variety of computer languages, many of which are obsolete. Some applications include thousands, tens of thousands, or even millions of lines of code, each of which must be examined for date-format problems.

To meet this challenge and monitor individual agency efforts, the Office of Management and Budget (OMB) directed the major departments and agencies to submit quarterly reports on their progress, beginning May 15, 1997. These reports contain information on where agencies stand with respect to the assessment, renovation, validation, and implementation of mission-critical systems, as well as other management information on items such as costs and business continuity and contingency plans.

The federal government's most recent reports show improvement in addressing the Year 2000 problem. While much work remains, the federal government has significantly increased its percentage of mission-critical systems that are reported to be Year 2000 compliant, as chart 1 illustrates. In particular, while the federal government did not meet its goal of having all mission-critical systems compliant by March 1999, as of mid-May 1999, 93 percent of these systems were reported compliant.

Chart 1: Mission-Critical Systems Reported Year 2000 Compliant, May 1997-May 1999



Source: May 1997 – May 1999 data are from the OMB quarterly reports.

While this reported progress is notable, OMB also noted that 10 agencies have mission-critical systems that were not yet compliant.[7] In addition, as we testified in April, some of the systems that were not yet compliant support vital government functions.[8] For example, some of the systems that were not compliant were among the 26 mission-critical systems that the Federal Aviation Administration (FAA) has identified as posing the greatest risk to the National Airspace System—the network of equipment, facilities, and information that supports U.S. aviation operations.

Additionally, not all systems have undergone an independent verification and validation process. For example, in April 1999 the Department of Commerce awarded a contract for independent verification and validation reviews of approximately 40 mission-critical systems that support that Department's most critical business processes. These reviews are to continue through the summer of 1999. In some cases, independent verification and validation of compliant systems have found serious problems. For example, as we testified this past February,[9] none of 54 external mission-critical systems of the Health Care Financing Administration reported by the Department of Health and Human Services (HHS) as compliant as of December 31, 1998, was Year 2000 ready at that time, based on serious qualifications identified by the independent verification and validation contractor.

Reviews Show Uneven Federal Agency Progress

While the overall Year 2000 readiness of the government has improved, our reviews of federal agency Year 2000 programs have found uneven progress. Some agencies had made good progress while other agencies were significantly behind schedule but had taken actions to improve their readiness. For example:

- In October 1997, we reported that while SSA had made significant progress in assessing and renovating mission-critical mainframe software, certain areas of risk in its Year 2000 program remained.[10] Accordingly, we made several recommendations to address these risk areas, which included the Year 2000 compliance of the systems used by the 54 state Disability Determination Services[11] that help administer the disability programs. SSA agreed with these recommendations and, in July 1999, we

[7] The 10 agencies were the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Justice, Transportation, Treasury; the National Aeronautics and Space Administration; and the U.S. Agency for International Development.

[8] Year 2000 Computing Challenge: Federal Government Making Progress But Critical Issues Must Still Be Addressed to Minimize Disruptions (GAO/T-AIMD-99-144, April 14, 1999).

[9] Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services (GAO/T-AIMD-99-92, February 26, 1999).

[10] Social Security Administration: Significant Progress Made in Year 2000 Effort, But Key Risks Remain (GAO/AIMD-98-6, October 22, 1997).

[11] These include the systems in all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.

reported that actions to implement these recommendations had either been taken or were underway.[12] For example, regarding the state Disability Determination Services systems, SSA enhanced its monitoring and oversight by establishing a full-time project team, designating project managers and coordinators, and requesting bi-weekly reports. While actions such as these demonstrated SSA's leadership in addressing the Year 2000 problem, it still needed to complete critical tasks to ensure readiness, including (1) ensuring the compliance of all external data exchanges, (2) completing tasks outlined in its contingency plans, (3) certifying the compliance of one remaining mission-critical system, (4) completing hardware and software upgrades in the Office of Telecommunications and Systems Operations, and (5) correcting date field errors identified through its quality assurance process.

- In May 1999 we testified[13] that the Department of Education had made progress toward addressing the significant risks we had identified in September 1998[14] related to systems testing, exchanging data with internal and external partners, and developing business continuity and contingency plans. Nevertheless, work remained ongoing in these areas. For example, Education had scheduled a series of tests with its data exchange partners, such as schools, through the early part of the fall. Tests such as these are important since Education's student financial aid environment is very large and complex, including over 7,000 schools, 6,500 lenders, and 36 guaranty agencies, as well as other federal agencies; we have reported that Education has experienced serious data integrity problems in the past.[15] Accordingly, our May testimony stated that Education needed to continue end-to-end testing of critical business processes involving Education's internal systems and its external data exchange partners and continue its outreach activities with schools, guaranty agencies, and other participants in the student financial aid community.

- Our work has shown that the Department of Defense and the military services face significant problems.[16] This March we testified that, despite considerable progress made in the preceding 3 months, the Department of Defense was still well behind schedule.[17] We found that the department faced two significant challenges: (1)

[12] Social Security Administration: Update on Year 2000 and Other Key Information Technology Initiatives (GAO/T-AIMD-99-259, July 29, 1999).
[13] Year 2000 Computing Challenge: Education Taking Needed Actions But Work Remains (GAO/T-AIMD-99-180, May 12, 1999).
[14] Year 2000 Computing Crisis: Significant Risks Remain to Department of Education's Student Financial Aid Systems (GAO/T-AIMD-98-302, September 17, 1998).
[15] Student Financial Aid Information: Systems Architecture Needed to Improve Programs' Efficiency (GAO/AIMD-97-122, July 29, 1997).
[16] Defense Computers: Year 2000 Computer Problems Put Navy Operations At Risk (GAO/AIMD-98-150, June 30, 1998); Defense Computers: Army Needs to Greatly Strengthen Its Year 2000 Program (GAO/AIMD-98-53, May 29, 1998); GAO/AIMD-98-72, April 30, 1998; and Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998).
[17] Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed (GAO/T-AIMD-99-101, March 2, 1999).

completing remediation and testing of its mission-critical systems and (2) having a reasonable level of assurance that key processes will continue to work on a day-to-day basis and key operational missions necessary for national defense can be successfully accomplished. We concluded that such assurance could only be provided if Defense took steps to improve its visibility over the status of key business processes.

End-To-End Testing Must Be Completed

While it is important to achieve compliance for individual mission-critical systems, realizing such compliance alone does not ensure that business functions will continue to operate through the change of century—the ultimate goal of Year 2000 efforts. The purpose of end-to-end testing is to verify that a defined set of interrelated systems, which collectively support an organizational core business area or function, will work as intended in an operational environment. In the case of the year 2000, many systems in the end-to-end chain will have been modified or replaced. As a result, the scope and complexity of testing--and its importance--are dramatically increased, as is the difficulty of isolating, identifying, and correcting problems. Consequently, agencies must work early and continually with their data exchange partners to plan and execute effective end-to-end tests. (Our Year 2000 testing guide sets forth a structured approach to testing, including end-to-end testing.)[18]

In January we testified that with the time available for end-to-end testing diminishing, OMB should consider, for the government's most critical functions, setting target dates, and having agencies report against them, for the development of end-to-end test plans, the establishment of test schedules, and the completion of the tests.[19] On March 31, OMB and the Chair of the President's Council on Year 2000 Conversion announced that one of the key priorities that federal agencies will be pursuing during the rest of 1999 will be cooperative end-to-end testing to demonstrate the Year 2000 readiness of federal programs with states and other partners.

Agencies have also acted to address end-to-end testing. For example, our March FAA testimony[20] found that the agency had addressed our prior concerns about the lack of detail in its draft end-to-end test program plan and had developed a detailed end-to-end testing strategy and plans.[21] Also, in June 1999 we reported[22] that the Department of Defense had underway or planned hundreds of related Year 2000 end-to-end test and evaluation activities and that, thus far, it was taking steps to ensure that these related end-to-end tests were effectively coordinated. However, we concluded that the Department of

[18] GAO/AIMD-10.1.21, November 1998.

[19] Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, January 20, 1999).

[20] GAO/T-AIMD/RCED-99-118, March 15, 1999.

[21] GAO/T-AIMD-98-251, August 6, 1998.

[22] Defense Computers: Management Controls Are Critical To Effective Year 2000 Testing (GAO/AIMD-99-172, June 30, 1999).

Defense was far from successfully finishing its various Year 2000 end-to-end test activities and that it must complete efforts to establish end-to-end management controls, such as establishing an independent quality assurance program.

Business Continuity and Contingency Plans Are Needed

Business continuity and contingency plans are essential. Without such plans, when unpredicted failures occur, agencies will not have well-defined responses and may not have enough time to develop and test alternatives. Federal agencies depend on data provided by their business partners as well as on services provided by the public infrastructure (e.g., power, water, transportation, and voice and data telecommunications). One weak link anywhere in the chain of critical dependencies can cause major disruptions to business operations. Given these interdependencies, it is imperative that contingency plans be developed for all critical core business processes and supporting systems, regardless of whether these systems are owned by the agency. Accordingly, in April 1998 we recommended that the Council require agencies to develop contingency plans for all critical core business processes.[23]

OMB has clarified its contingency plan instructions and, along with the Chief Information Officers Council, has adopted our business continuity and contingency planning guide.[24] In particular, on January 26, 1999, OMB called on federal agencies to identify and report on the high-level core business functions that are to be addressed in their business continuity and contingency plans, as well as to provide key milestones for development and testing of such plans in their February 1999 quarterly reports. In addition, on May 13 OMB required agencies to submit high-level versions of these plans by June 15. According to an OMB official, OMB has received plans from the 24 major departments and agencies. This official stated that OMB planned to review the plans, discuss them with the agencies, determine whether there were any common themes, and report on the plans' status in its next quarterly report.

To provide assurance that agencies' business continuity and contingency plans will work if needed, on January 20 we suggested that OMB may want to consider requiring agencies to test their business continuity strategy and set a target date, such as September 30, 1999, for the completion of this validation.[25] Our review of the 24 major departments and agencies' May 1999 quarterly reports found 14 cases in which agencies did not identify test dates for their business continuity and contingency plans or reported test dates subsequent to September 30, 1999.

On March 31, OMB and the Chair of the President's Council announced that completing and testing business continuity and contingency plans as insurance against disruptions to federal service delivery and operations from Year 2000-related failures will be one of the

[23] Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Parternships (GAO/AIMD-98-85, April 30, 1998).

[24] GAO/AIMD-10.1.19, August 1998.

[25] GAO/T-AIMD-99-50, January 20, 1999.

key priorities that federal agencies will be pursuing through the rest of 1999. Accordingly, OMB should implement our suggestion and establish a target date for the validation of agency business continuity and contingency plans.

Our reviews of specific agency business continuity and contingency plans have found that agencies are in varying stages of completion. For example,

- We testified in July 1999 that SSA was in the process of testing all of its contingency plans, with expected completion in September.[26] In addition, SSA planned to assist the Department of the Treasury in developing alternative disbursement processes for problematic financial institutions.

- This June, we testified that the U. S. Customs Service had implemented sound management processes for developing business continuity and contingency plans and was in the process of testing its plans.[27] Customs expected to complete contingency plan testing by October 1999.

- In May 1999, we reported[28] that the Department of Agriculture's component agencies were actively engaged in developing business continuity and contingency plans but that much work remained to complete and test these plans. Further, its December 1999 departmentwide goal of completing business continuity and contingency plans left no room for delays or sufficient time for correcting, revising, and retesting plans, if necessary. Consequently, we recommended that the Department of Agriculture advance its time frame to no later than September 30, 1999, and develop priorities for completing and testing business continuity and contingency plans that are aligned with the department's highest priority business processes, to ensure that remaining work addresses these processes first. The Department of Agriculture's Chief Information Officer stated that the department planned to implement our recommendations.

- This June, we reported[29] that the General Services Administration had completed its telecommunications business continuity and contingency plan in September 1998. However, we made several suggestions for enhancing this plan, including that the General Services Administration work with its customers to ensure that the customers' business continuity and contingency plans are fully coordinated with the General Services Administration's plan and that it consider the possibility of partial loss of service. The General Services Administration agreed to implement our suggestions.

[26] GAO/T-AIMD-99-259, July 29, 1999.

[27] Year 2000 Computing Crisis: Customs Is Making Good Progress (GAO/T-AIMD-99-225, June 29, 1999).

[28] Year 2000 Computing Crisis: USDA Needs to Accelerate Time Frames for Completing Contingency Planning (GAO/AIMD-99-178, May 21, 1999).

[29] GSA's Effort to Develop Year 2000 Business Continuity and Contingency Plans for Telecommunications Systems (GAO/AIMD-99-201R, June 16, 1999).

OMB Action Could Help Ensure Business Continuity of High-Impact Programs

While individual agencies have been identifying and remediating mission-critical systems, the government's future actions need to be focused on its high-priority programs and ensuring the continuity of these programs, including the continuity of federal programs that are administered by states. Accordingly, governmentwide priorities need to be based on such criteria as the potential for adverse health and safety effects, adverse financial effects on American citizens, detrimental effects on national security, and adverse economic consequences. In April 1998 we recommended that the President's Council on Year 2000 Conversion establish governmentwide priorities and ensure that agencies set agencywide priorities.[30]

On March 26, OMB implemented our recommendation by issuing a memorandum to federal agencies designating lead agencies for the government's 42 high-impact programs (e.g., food stamps, Medicare, and federal electric power generation and delivery). (OMB later added a 43rd high-impact program—the Department of Justice's National Crime Information Center.) Appendix I lists these programs and their lead agencies. For each program, the lead agency was charged with identifying to OMB the partners integral to program delivery; taking a leadership role in convening those partners; assuring that each partner has an adequate Year 2000 plan and, if not, helping each partner without one; and developing a plan to ensure that the program will operate effectively. According to OMB, such a plan might include testing data exchanges across partners, developing complementary business continuity and contingency plans, sharing key information on readiness with other partners and the public, and taking other steps necessary to ensure that the program will work. OMB directed the lead agencies to provide a schedule and milestones of key activities in their plans by April 15. OMB also asked agencies to provide monthly progress reports. As you know, we are currently reviewing agencies' progress in ensuring the readiness of their high-impact programs for this subcommittee.

STATE AND LOCAL GOVERNMENTS FACE SIGNIFICANT YEAR 2000 RISKS

Just as the federal government faces significant Year 2000 risks, so too do state and local governments. If the Year 2000 problem is not properly addressed, for example, (1) food stamps and other types of payments may not be made or could be made for incorrect amounts; (2) date-dependent signal timing patterns could be incorrectly implemented at highway intersections, with safety severely compromised; and (3) prisoner release or parole eligibility determinations may be adversely affected. Nevertheless, available information on the Year 2000 readiness of state and local governments indicates that much work remains.

[30] GAO/AIMD-98-85, April 30, 1998.

According to information on state Year 2000 activities reported to the National Association of State Information Resource Executives as of August 3, 1999,[31] states[32] reported having thousands of mission-critical systems.[33] With respect to completing the implementation phase for these systems,

- 2 states[34] reported that they had completed between 25 and 49 percent,
- 6 states[35] reported completing between 50 and 74 percent,
- 38 states[36] reported completing between 75 and 99 percent, and
- 3 states reported completing the implementation phase for all mission-critical systems.[37]

All of the states responding to the National Association of State Information Resource Executives survey reported that they were actively engaged in internal and external contingency planning and that they had established target dates for the completion of these plans; 14 (28 percent) reported the deadline as October 1999 or later.

State audit organizations have also identified significant Year 2000 concerns. In January, the National State Auditors Association reported on the results of its mid-1998 survey of Year 2000 compliance among states.[38] This report stated that, for the 12 state audit organizations that provided Year 2000-related reports, concerns had been raised in areas such as planning, testing, embedded systems, business continuity and contingency planning, and the adequacy of resources to address the problem.

We identified additional products by 17 state-level audit organizations and Guam that

[31] Individual states submit periodic updates to the National Association of State Information Resource Executives. For the August 3 report, over three quarters of the states submitted their data after July 1, 1999. The oldest data were provided on March 11 and the most recent data on August 2.

[32] In the context of the National Association of State Information Resource Executives survey, the term "states" includes the District of Columbia and Puerto Rico.

[33] Mission-critical systems were defined as those that a state had identified as priorities for prompt remediation.

[34] One state reported on its mission-critical systems and one state reported on its processes.

[35] Five states reported on their mission-critical systems and one reported on all systems.

[36] Thirty-one states reported on their mission-critical systems, two states reported on their applications, one reported on its "priority business activities," one reported on its "critical compliance units," one reported on all systems, one reported on functions, and one reported on projects.

[37] Two states did not respond to the survey and one did not respond to this question.

[38] Year 2000: State Compliance Efforts (National State Auditors Association, January 1999).

discussed the Year 2000 problem and that had been issued since October 1, 1998. Several of these state-level audit organizations noted that progress had been made. However, the audit organizations also expressed concerns that were consistent with those reported by the National State Auditors Association. For example:

- In December 1998 the Vermont State Auditor reported[39] that the state Chief Information Officer did not have a comprehensive control list of the state's information technology systems. Accordingly, the audit office stated that, even if all mission-critical state systems were checked, these systems could be endangered by information technology components that had not been checked or by linkages with the state's external electronic partners.

- In April, New York's Division of Management Audit and State Financial Services reported that state agencies did not adequately control the critical process of testing remediated systems.[40] Further, most agencies were in the early stages of addressing potential problems related to data exchanges and embedded systems and none had completed substantive work on contingency planning. The New York audit office subsequently issued 27 reports on individual mission-critical and high-priority systems that included concerns about, for example, contingency planning and testing.

- In August, the Mississippi Office of the State Auditor reported that while some state agencies had developed limited contingency plans, others had not done so.[41]

- In March, North Carolina's State Auditor reported[42] that resource restrictions had limited the state's Year 2000 Project Office's ability to verify data reported by state agencies.

With respect to California, in February, the California State Auditor reported[43] that state agencies were making progress in ensuring the uninterrupted delivery of critical services but that many of the 14 agencies that provide the most critical services had not completed their Year 2000 efforts. Eleven agencies had not completely tested their computer systems and seven had not corrected or replaced embedded systems. For example, key

[39] Vermont State Auditor's Report on State Government's Year 2000 Preparedness (Y2K Compliance) for the Period Ending November 1, 1998 (Office of the State Auditor, December 31, 1998).

[40] New York's Preparation for the Year 2000: A Second Look (Office of the State Comptroller, Division of Management Audit and State Financial Services, Report 98-S-21, April 5, 1999).

[41] A Performance Review of the Year 2000 (Y2K) Computer Problem: State and Local Government (Office of the State Auditor, State of Mississippi, August 5, 1999).

[42] Department of Commerce, Information Technology Services Year 2000 Project Office (Office of the State Auditor, State of North Carolina, March 18, 1999).

[43] Year 2000 Computer Problem: The State's Agencies Are Progressing Toward Compliance but Key Steps Remain Incomplete (California State Auditor, February 18, 1999).

agencies responsible for emergency services, corrections, and water resources had not fully addressed embedded technology-related threats. Regarding emergency services, the California report stated that if remediation of the embedded technology in its networks were not completed, the Office of Emergency Services might have to rely on cumbersome manual processes, significantly increasing response time to disasters.

It is also essential that local government systems be ready for the change of century since critical functions involving, for example, public safety and traffic management, are performed at the local level. Recent reports on local governments have highlighted Year 2000 concerns. For example:

- On July 15, we reported on the reported Year 2000 status of the 21 largest U.S. cities.[44] On average, cities reported completing work for 45 percent of the key service areas in which they have responsibility. In addition, two cities reported that they had completed their Year 2000 efforts, nine cities expected to complete their Year 2000 preparations by September 30, 1999, and the remaining 10 cities expected to complete their preparation by December 31.[45] In addition, 7 cities reported completing Year 2000 contingency plans, while 14 cities reported that their plans were still being developed.

- On July 9, the National League of Cities reported on its survey of 403 cities conducted in April 1999. This survey found that (1) 92 percent of cities had a citywide Year 2000 plan, (2) 74 percent had completed their assessment of critical systems, and (3) 66 percent had prepared contingency plans. (Of those that had not completed such plans, about half stated that they were planning to develop one.) In addition, 92 percent of the cities reported that they expect that all of their critical systems will be compliant by January 1, 2000; 5 percent expected to have completed between 91 and 99 percent, and 3 percent expected to have completed between 81 and 90 percent of their critical systems by January 1.

- On June 23, the National Association of Counties announced the results of its April survey of 500 randomly selected counties. This survey found that (1) 74 percent of respondents had a countywide plan to address Year 2000 issues, (2) 51 percent had completed system assessments, and (3) 27 percent had completed system testing. In addition, 190 counties had prepared contingency plans and 289 had not. Further, of the 114 counties reporting that they planned to develop Year 2000 contingency plans, 22 planned to develop the plan in April-June, 64 in July-September, 18 in October-December, and 10 did not yet know.

[44] Reported Y2K Status of the 21 Largest U.S. Cities (GAO/AIMD-99-246R, July 15, 1999).

[45] In most cities, the majority of city services are scheduled to be completed before this completion date. For example, Los Angeles plans to have all key city systems ready by September 30, except for its wastewater treatment systems, which are expected to be completed in November.

Of critical importance to the nation are services essential to the safety and well-being of individuals across the country, namely 9-1-1 systems and law enforcement. For the most part, responsibility for ensuring continuity of service for 9-1-1 calls and law enforcement resides with thousands of state and local jurisdictions. On April 29 we testified that not enough was known about the status of either 9-1-1 systems or of state and local law enforcement activities to conclude about either's ability during the transition to the year 2000 to meet the public safety and well-being needs of local communities across the nation.[46] While the federal government planned additional actions to determine the status of these areas, we stated that the President's Council on Year 2000 Conversion should use such information to identify specific risks and develop appropriate strategies and contingency plans to respond to those risks.

We subsequently reported[47] that the Federal Emergency Management Agency and the Department of Justice have worked to increase the response rate to a survey of public safety organizations. As of June 30, 1999, of the over 2,200 9-1-1 sites responding, 37 percent reported that they were ready for the Year 2000. Another 55 percent responded that they expected to be Year 2000 compliant in time for the change of century.

Recognizing the seriousness of the Year 2000 risks facing state and local governments, the President's Council has developed initiatives to address the readiness of state and local governments. For example:

- The Council established working groups on state and local governments and tribal governments.
- Council officials participate in monthly multistate conference calls.
- In July 1998 and March 1999, the Council, in partnership with the National Governors' Association, convened Year 2000 summits with state and U.S. territory Year 2000 coordinators.
- On May 24, the Council announced a nationwide campaign to promote "Y2K Community Conversations" to support and encourage efforts of government officials, business leaders, and interested citizens to share information on their progress. To support this initiative, the Council has developed and is distributing a toolkit that provides examples of which sectors should be represented at these events and issues that should be addressed.

[46] Year 2000 Computing Challenge: Status of Emergency and State and Local Law Enforcement Systems Is Still Unknown (GAO/T-AIMD-99-163, April 29, 1999).
[47] Emergency and State and Local Law Enforcement Systems: Committee Questions Concerning Year 2000 Challenges (GAO/AIMD-99-247R, July 14, 1999).

State-Administered Federal Human Services Programs Are At Risk

Among the critical functions performed by states are the administration of federal human services programs. As we reported in November 1998, many systems that support state-administered federal human services programs were at risk, and much work remained to ensure that services would continue.[48] In February of this year, we testified that while some progress had been achieved, many states' systems were not scheduled to become compliant until the last half of 1999.[49] Accordingly, we concluded that, given these risks, business continuity and contingency planning was even more important in ensuring continuity of program operations and benefits in the event of systems failures.

Subsequent to our November 1998 report, OMB directed federal oversight agencies to include the status of selected state human services systems in their quarterly reports. Specifically, in January 1999, OMB requested that agencies describe actions to help ensure that federally supported, state-run programs will be able to provide services and benefits. OMB further asked that agencies report the date when each state's systems will be Year 2000-compliant.

Table 1 summarizes the latest information on state-administered federal human services programs reported by OMB on June 15, 1999.[50] This information was gathered, but not verified, by the Departments of Agriculture, HHS, and Labor.[51] It indicates that while many states reported their programs to be compliant, a number of states did not plan to complete Year 2000 efforts until the last quarter of 1999. For example, eight states did not expect to be compliant until the last quarter of 1999 for Child Support Enforcement, five states for Unemployment Insurance, and four states for Child Nutrition. Moreover, Year 2000 readiness information was unknown in many cases. For example, according to OMB, the status of 32 states' Low Income Home Energy Assistance programs was unknown because applicable readiness information was not available.

[48] Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998).

[49] Year 2000 Computing Crisis: Readiness of State Automated Systems That Support Federal Human Services Programs (GAO/T-AIMD-99-91, February 24, 1999).

[50] For Medicaid, OMB reports on the two primary systems that states use to administer the program: (1) the Integrated Eligibility System, to determine whether an individual applying for Medicaid meets the eligibility criteria for participation, and (2) the Medicaid Management Information System, to process claims and deliver payments for services rendered. Integrated eligibility systems are also often used to determine eligibility for other public assistance programs, such as Food Stamps.

[51] The Department of Agriculture oversees the Child Nutrition, Food Stamp, and the Women, Infants, and Children programs. HHS oversees the Child Care, Child Support Enforcement, Child Welfare, Low Income Home Energy Assistance, Medicaid, and Temporary Assistance for Needy Families programs. The Department of Labor oversees the Unemployment Insurance program.

Table 1: Reported State-level Readiness for Federally Supported Programs[a]

Program[b]	Compliant[c]	Expected Date of 1999 Compliance				Unk.[d]	N/A[e]
		Jan.-March	April-June	July-Sept.	Oct.-Dec.		
Child Nutrition	29	0	9	10	4	2	0
Food Stamps	25	0	12	14	3	0	0
Women, Infants, and Children	33	0	11	7	3	0	0
Child Care	24	5	5	8	2	6	4
Child Support Enforcement	15	4	13	8	8	6	0
Child Welfare	20	5	9	11	3	5	1
Low Income Home Energy Assistance Program	10	0	3	7	1	32	1
Medicaid – Integrated Eligibility System	20	0	15	15	4	0	0
Medicaid – Management Information System	17	0	19	14	4	0	0
Temporary Assistance for Needy Families	19	3	12	15	1	4	0
Unemployment Insurance	27	0	11	10	5	0	1

[a] This chart contains readiness information from the 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.

[b] According to OMB, the information regarding Child Care, Child Support Enforcement, the Low Income Home Energy Assistance Program, Medicaid, and Temporary Assistance for Needy Families was as of January 31, 1999; and the information for Child Nutrition, Food Stamps, and Women, Infants and Children was as of March 1999. However, OMB provided a draft table to the National Association of State Information Resource Executives which, in turn, provided the draft table to the states. The states were asked to contact HHS and Agriculture and provide corrections by June 1, 1999. For their part, HHS and Agriculture submitted updated state data to OMB in early June. The information regarding Unemployment Insurance was as of March 31, 1999.

[c] In many cases, the report indicated a date instead of whether the state was compliant. We assumed that states reporting completion dates in 1998 or earlier were compliant.

[d] Unknown indicates that, according to OMB, the data reported by the states were unclear or that no information was reported by the agency.

[e] N/A indicates that the states or territories reported that the data requested were not applicable to them.

Source: Progress on Year 2000 Conversion: 9th Quarterly Report (OMB, issued on June 15, 1999).

Although many states have reported their state-administered programs to be compliant, additional work beyond individual system completion likely remains, such as end-to-end testing. For example, of the states that OMB reported as having compliant Medicaid management information and/or integrated eligibility systems, at least four and five states, respectively, had not completed end-to-end testing.

In addition to obtaining state-reported readiness status information for OMB, the three federal departments are taking other actions to assess the ability of state-administered programs to continue into the next century. However, as table 2 shows, the approaches of the three departments in assessing the readiness of state-administered federal human services programs vary significantly. For example, HHS' Health Care Financing Administration (HCFA) hired a contractor to perform comprehensive on-site reviews in all states, some more than once, using a standard methodology. Agriculture's Food and Nutrition Service (FNS) approach includes such actions as having regional offices monitor state Year 2000 efforts and obtaining state certifications of compliance. The Department of Labor is relying on its regional offices to monitor state Year 2000 efforts as well as requiring states to obtain and submit an independent verification and validation report after declaring their systems compliant.

Table 2: Number and Types Of Assessments Performed

		Areas Covered By Assessments		
Agency/ Program	Number of States Assessed	Project Management/ Planning	Test Plans/ Results	Business Continuity and Contingency Plans (BCCP)
Agriculture/ Child Nutrition Program	Component entity's regional offices are monitoring all states' efforts	Varies by region	Varies by region	Varies by region
Agriculture/ Food Stamps	Component entity's regional offices are monitoring all states' efforts	Varies by region	Varies by region	Varies by region
Agriculture/ Women, Infants, and Children	Component entity's regional offices are monitoring all states' efforts	Varies by region	Varies by region	Varies by region
HHS/Child Care	As of July 2, a contractor had conducted on-site reviews of 20 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—on-site visits included reviews of states' BCCP processes, but not their content
HHS/Child Support Enforcement	As of July 2, a contractor had conducted on-site reviews of 20 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—on-site visits included reviews of states' BCCP processes, but not their content
HHS/Child Welfare	As of July 2, a contractor had conducted on-site reviews of 20 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—on-site visits included reviews of states' BCCP processes, but not their content
HHS/Low Income Housing Energy Assistance Program	As of July 2, a contractor had conducted on-site reviews of 20 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—on-site visits included reviews of states' BCCP processes, but not their content
HHS/Medicaid	A contractor conducted on-site reviews of 50 states and the District of Columbia once, and as of June 30, the contractor had conducted follow-up reviews of 14 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—Initial visits included a review of a state's BCCP process, and as of July 9, a contractor had reviewed the content of 42 states' BCCPs, either on site or at headquarters
HHS/ Temporary Assistance for Needy Families	As of July 2, a contractor had conducted on-site reviews of 20 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—on-site visits included reviews of states' BCCP processes, but not their content
Labor/ Unemployment Insurance	Labor's regional offices are monitoring all states' efforts	Unknown—not specifically addressed in methodology	Unknown—not specifically addressed in methodology	Reviews ongoing

In addition to the completed reviews, all of the departments have ongoing initiatives to ensure that state-administered human services programs will continue to function past the change of century. These initiatives are part of the departments' overall strategies to ensure the continued delivery of these high-impact programs. For example,

- In June 1999, the Department of Agriculture's FNS required its regions to provide for each program a copy of either a state letter certifying that it was Year 2000 compliant or a business continuity and contingency plan. As of June 18, 1999, FNS had received (1) 9 certifications and 7 business continuity and contingency plans for Child Nutrition; (2) 12 certifications and 16 business continuity and contingency plans for Food Stamps; and (3) 23 certifications and 23 business continuity and contingency plans for Women, Infants, and Children. In addition, to help states' Year 2000 efforts, FNS employed a contractor to conduct on-site visits to 20 states for one or more programs. As of July 9, FNS officials told us 16 states had been visited. With respect to the scope of these visits, FNS' regional offices determine for each state and program what specific areas it should encompass. These visits are principally intended to provide technical assistance to the states in areas such as Year 2000 project management, hardware and software testing, and contingency planning.

- In its initial round of on-site reviews conducted between November 1998 and April 1999, the contractor hired by HHS' HCFA (1) identified barriers to successful remediation; (2) made recommendations to address specific areas of concern; and (3) placed Medicaid integrated eligibility and management information systems into low, medium, or high risk categories. HCFA's contractor is currently conducting a second round of on-site reviews in at least 40 states—primarily those in which at least one of two systems was categorized as a high or medium risk during the initial visit. As of June 30, 14 states had been visited during this round. The focus of this second round of visits is on determining how states have resolved Year 2000 issues previously identified, as well as reviewing activities such as data exchanges and end-to-end testing. HCFA plans to conduct a third round of on-site reviews in the fall of 1999 for those states that continue to have systems categorized as high risk. Additionally, another HCFA contractor is reviewing the content of all states' business continuity and contingency plans, with some of these reviews being performed in conjunction with the second round of state visits.

- In September 1998, the Department of Labor required that all State Employment Security Agencies conduct independent verification and validation reviews of their Unemployment Insurance programs. The department set a target date of July 1, 1999, for states to submit independent verification and validation certifications of their Unemployment Insurance systems to Labor's regional offices. Labor required its regional offices to review independent verification and validation reports and certifications of Year 2000 compliance that State Employment Security Agencies submitted, and ascertain whether the material met the department's requirements. If Labor's requirements were met, the regional offices were to approve the State Employment Security Agencies' certification and independent verification and validation reports and forward copies of the approved certification and report, along

with regional office comments, to Labor's national office.

An example of the benefits that federal/state partnerships can provide is illustrated by the Department of Labor's unemployment services program. In September 1998, we reported that many State Employment Security Agencies were at risk of failure as early as January 1999 and urged the Department of Labor to initiate the development of realistic contingency plans to ensure continuity of core business processes in the event of Year 2000-induced failures.[52] In May, we testified that four state agencies' systems could have failed if systems in those states had not been programmed with an emergency patch in December 1998. This patch was developed by several of the state agencies and promoted to other state agencies by the Department of Labor. [53]

YEAR 2000 READINESS INFORMATION AVAILABLE IN SOME SECTORS, BUT KEY INFORMATION STILL MISSING OR INCOMPLETE

Beyond the risks faced by federal, state, and local governments, the year 2000 also poses a serious challenge to the public infrastructure, key economic sectors, and to other countries. To address these concerns, in April 1998 we recommended that the Council use a sector-based approach and establish the effective public-private partnerships necessary to address this issue.[54] The Council subsequently established over 25 sector-based working groups and has been initiating outreach activities since it became operational last spring. In addition, the Chair of the Council has formed a Senior Advisors Group composed of representatives from private-sector firms across key economic sectors. Members of this group are expected to offer perspectives on cross-cutting issues, information sharing, and appropriate federal responses to potential Year 2000 failures.

Our April 1998 report also recommended that the President's Council develop a comprehensive picture of the nation's Year 2000 readiness, to include identifying and assessing risks to the nation's key economic sectors--including risks posed by international links. In October 1998 the Chair directed the Council's sector working groups to begin assessing their sectors. The Chair also provided a recommended guide of core questions that the Council asked to be included in surveys by the associations performing the assessments. These questions included the percentage of work that has been completed in the assessment, renovation, validation, and implementation phases. The Chair then planned to issue quarterly public reports summarizing these assessments.

[52] Year 2000 Computing Crisis: Progress Made at Department of Labor, But Key Systems at Risk (GAO/T-AIMD-98-303, September 17, 1998).
[53] Year 2000 Computing Challenge: Labor Has Progressed But Selected Systems Remain at Risk (GAO/T-AIMD-99-179, May 12, 1999).
[54] GAO/AIMD-98-85, April 30, 1998.

The Council's most recent report was issued on August 5, 1999.[55] The report stated that important national systems will make a successful transition to the year 2000 but that much work, such as contingency planning, remains to be done. In particular, the Council expressed a high degree of confidence in five major domestic areas: financial institutions, electric power, telecommunications, air travel, and the federal government. For example, the Council stated that on August 2, federal bank, thrift, and credit union regulators reported that 99 percent of federally insured financial institutions have completed testing of critical systems for Year 2000 readiness. The Council had concerns in four significant areas: local government, health care, education, and small businesses. For example, according to the Council report, many school districts could move into the new century with dysfunctional information technology systems, since only 28 percent and 30 percent of Superintendent/Local Educational Agencies and post-secondary institutions, respectively, reported that their mission-critical systems were Year 2000 compliant. Internationally, the Council stated that the Year 2000 readiness of other countries was improving but was still a concern. The Council reported that the June 1999 meeting of National Year 2000 Coordinators held at the United Nations found that the 173 countries in attendance were clearly focused on the Year 2000 problem but that many countries will likely not have enough time or resources to finish before the end of 1999.

The Council's assessment reports have substantially increased the nation's understanding of the Year 2000 readiness of key industries. However, the picture remains incomplete in certain key areas because the surveys conducted to date did not have a high response rate or did not provide their response rate; the assessment was general or contained projections rather than current remediation information; or the data were old. For example, according to the Council's latest assessment report,

- Less than a quarter of the more than 16,000 Superintendents of Schools/Local Educational Agencies responded to a web-based survey of Year 2000 readiness among elementary and secondary schools. Similarly, less than a third of the more than 6,000 presidents and/or chancellors of post-secondary educational institutions responded to a web-based Year 2000 survey. Also, surveys covering areas such as small and medium-sized chemical enterprises did not provide information on either the number of surveys distributed or the number returned. Small response rates or the lack of information on response rates call into question whether the results of the survey accurately portray the readiness of the sector.

- Information in areas, such as state emergency management and broadcast television and radio provided a general assessment or projected compliance levels as of a certain date, but did not contain detailed data as to the current status of the sector (e.g., the average percentage of organizations' systems that are Year 2000 compliant or the

[55] The Council's three reports are available on its web site, *www.y2k.gov*. In addition, the Council, in conjunction with the Federal Trade Commission and the General Services Administration, has established a toll-free Year 2000 information line, 1-888-USA-4Y2K. The Federal Trade Commission has also included Year 2000 information of interest to consumers on its web site, *www.consumer.gov*.

percentage of organizations that are in the assessment, renovation, or validation phases).

- In some cases, such as for grocery manufacturers, cable television, hospitals, physicians' practices, and railroads, the sector surveys had been conducted months earlier and/or current survey information was not yet available.

In addition to our work related to the federal, state, and local government's Year 2000 progress, we have also issued several products related to key economic sectors. I will now discuss the results of these reviews.

Energy Sector

In April, we reported that while the electric power industry had concluded that it had made substantial progress in making its systems and equipment ready to continue operations into the year 2000, significant risks remained since many reporting organizations did not expect to be Year 2000 ready within the June 1999 industry target date.[56] We, therefore, suggested that the Department of Energy (1) work with the Electric Power Working Group to ensure that remediation activities were accelerated for the utilities that expected to miss the June 1999 deadline for achieving Year 2000 readiness and (2) encourage state regulatory utility commissions to require a full public disclosure of Year 2000 readiness status of entities transmitting and distributing electric power. The Department of Energy generally agreed with our suggestions. We also suggested that the Nuclear Regulatory Commission (1) in cooperation with the Nuclear Energy Institute, work with nuclear power plant licensees to accelerate the Year 2000 remediation efforts among the nuclear power plants that expect to meet the June 1999 deadline for achieving readiness and (2) publicly disclose the Year 2000 readiness of each of the nation's operational nuclear reactors. In response, the Nuclear Regulatory Commission stated that it plans to focus its efforts on nuclear power plants that may miss the July 1, 1999 milestone and that it would release the readiness information on individual plants that same month.

Subsequent to our report, on August 3, 1999, the North American Electric Reliability Council released its fourth status report on electric power systems. According to the Council, as of June 30, 1999—the industry target date for organizations to be Year 2000 ready—251 of 268 (94 percent) of bulk electric organizations were Year 2000 ready or Year 2000 ready with limited exceptions.[57] In addition, this report stated that 96 percent

[56] Year 2000 Computing Crisis: Readiness of the Electric Power Industry (GAO/AIMD-99-114, April 6, 1999).

[57] The North American Electric Reliability Council reported that 64 of these organizations had exceptions but that it "believes that the work schedule provided to complete these exception items in the next few months represents a prudent use of resources and does not increase risks associated with reliable electric service into the Year 2000."

of local distribution systems were reported as Year 2000 ready.[58] The North American Electric Reliability Council stated that the information it uses is principally self-reported but that 84 percent of the organizations reported that their Year 2000 programs had also been audited by internal and/or external auditors. On July 19, the Nuclear Regulatory Commission stated that 68 of 103 (66 percent) nuclear power plants reported that all of their computer systems and digital embedded components that support plant operations are Year 2000 ready. Of the 35 plants that were not Year 2000 ready, 18 had systems or components that were not ready that could affect power generation.

In May, we reported[59] that while the domestic oil and gas industries had reported that they had made substantial progress in making their equipment and systems ready to continue operations into the year 2000, risks remained. For example, although over half of our oil is imported, little was known about the Year 2000 readiness of foreign oil suppliers. Further, while individual domestic companies reported that they were developing Year 2000 contingency plans, there were no plans to perform a national-level risk assessment and develop contingency plans to deal with potential shortages or disruptions in the nation's overall oil and gas supplies. We suggested that the Council's oil and gas working group (1) work with industry associations to perform national-level risk assessments and develop and publish credible, national-level scenarios regarding the impact of potential Year 2000 failures and (2) develop national-level contingency plans. The working group generally agreed with these suggestions.

Water Sector

In April we reported[60] that insufficient information was available to assess and manage Year 2000 efforts in the water sector, and little additional information was expected under the current regulatory approach. While the Council's water sector working group had undertaken an awareness campaign and had urged national water sector associations to continue to survey their memberships, survey response rates had been low. Further, Environmental Protection Agency officials stated that the agency lacked the rules and regulations necessary to require water and wastewater facilities to report on their Year 2000 status.

Our survey of state regulators found that a few states were proactively collecting Year 2000 compliance data from regulated facilities, a much larger group of states was disseminating Year 2000 information, while another group was not actively using either approach. Additionally, only a handful of state regulators believed that they were

[58] This was based on the percentage of the total megawatts of the systems reported as Year 2000 ready by investor-owned, public power, and cooperative organizations. The report did not identify the number of local distribution organizations that reported that they were Year 2000 ready.

[59] Year 2000 Computing Crisis: Readiness of the Oil and Gas Industries (GAO/AIMD-99-162, May 19, 1999).

[60] Year 2000 Computing Crisis: Status of the Water Industry (GAO/AIMD-99-151, April 21, 1999).

responsible for ensuring facilities' Year 2000 compliance or overseeing facilities' business continuity and contingency plans. Among our suggested actions was that the Council, the Environmental Protection Agency, and the states determine which regulatory organization should take responsibility for assessing and publicly disclosing the status and outlook of water sector facilities' Year 2000 business continuity and contingency plans. The Environmental Protection Agency generally agreed with our suggestions but one official noted that additional legislation may be needed if the agency is to take responsibility for overseeing facilities' Year 2000 business continuity and contingency plans.

Health Sector

The health sector includes health care providers (such as hospitals and emergency health care services), insurers (such as Medicare and Medicaid), and biomedical equipment. Last month we reported[61] that HCFA had taken aggressive and comprehensive outreach efforts with regard to its over 1.1 million healthcare providers that administer services for Medicare-insured patients.[62] Despite these efforts, HCFA data show that provider participation in its outreach activities has been low. Further, although HCFA has tasked contractors that process Medicare claims with testing with providers using future-dated claims, such testing had been limited and the testing that had occurred had identified problems. Our July report also found that although many surveys had been completed in 1999 on the Year 2000 readiness of healthcare providers; none of the 11 surveys we reviewed provided sufficient information with which to assess the Year 2000 status of the healthcare provider community. Each of the surveys had low response rates, and several did not address critical questions about testing and contingency planning.

To reduce the risk of Year 2000-related failures in the Medicare provider community, our July report suggested, for example, that HCFA consider using additional outreach methods, such as public service announcements, and set milestones for Medicare contractors for testing with providers. We also made suggestions to the President's Council on Year 2000 Conversion's healthcare sector working group, including a suggestion to consider working with associations to publicize those providers who respond to future surveys in order to increase survey response rates. The HCFA Administrator generally agreed with our suggested actions.

With respect to biomedical equipment, on June 10 we testified[63] that, in response to our September 1998 recommendation,[64] HHS, in conjunction with the Department of

[61] Year 2000 Computer Crisis: Status of Medicare Providers Unknown (GAO/AIMD-99-243, July 28, 1999).

[62] Examples of such providers are hospitals, laboratories, physicians, and skilled nursing/long term care facilities.

[63] Year 2000 Computing Challenge: Concerns About Compliance Information on Biomedical Equipment (GAO/T-AIMD-99-209, June 10, 1999).

[64] Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown (GAO/AIMD-98-240, September 18, 1998).

Veterans Affairs, had established a clearinghouse on biomedical equipment. As of June 1, 1999, 4,142 biomedical equipment manufacturers had submitted data to the clearinghouse. About 61 percent of these manufacturers reported having products that do not employ dates and about 8 percent (311 manufacturers) reported having date-related problems such as an incorrect display of date/time. According to the Food and Drug Administration, the 311 manufacturers reported 897 products with date-related problems. However, not all compliance information was available on the clearinghouse because the clearinghouse referred the user to 427 manufacturers' web sites. Accordingly, we reviewed the web sites of these manufacturers and found, as of June 1, 1999, a total of 35,446 products.[65] Of these products, 18,466 were reported as not employing a date, 11,211 were reported as compliant, 4,445 were shown as not compliant, and the compliance status of 1,324 was unknown.

In addition to the establishment of a clearinghouse, our September 1998 report[66] also recommended that HHS and the Department of Veterans Affairs take prudent steps to jointly review manufacturers' test results for critical care/life support biomedical equipment. We were especially concerned that the departments review test results for equipment previously deemed to be noncompliant but now deemed by manufacturers to be compliant, or equipment for which concerns about compliance remained. In May 1999, the Food and Drug Administration, a component agency of HHS, announced that it planned to develop a list of critical care/life support medical devices and the manufacturers of these devices, select a sample of manufacturers for review, and hire a contractor to develop a program to assess manufacturers' activities to identify and correct Year 2000 problems for these medical devices. In addition, if the results of this review indicated a need for further review of manufacturer activities, the contractor would review a portion of the remaining manufacturers not yet reviewed. Moreover, according to the Food and Drug Administration, any manufacturer whose quality assurance system appeared deficient based on the contractors review would be subject to additional reviews to determine what actions would be required to eliminate any risk posed by noncompliant devices.

In April testimony[67] we also reported on the results of a Department of Veterans Affairs survey of 384 pharmaceutical firms and 459 medical-surgical firms with whom it does business. Of the 52 percent of pharmaceutical firms that responded to the survey, 32 percent reported that they were compliant. Of the 54 percent of the medical-surgical firms that responded, about two-thirds reported that they were compliant.

[65] Because of limitations in many of the manufacturers web sites, our ability to determine the total number of biomedical equipment products reported and their compliance status was impaired. Accordingly, the actual number of products reported by the manufacturers could be significantly higher than the 35,446 products that we counted.

[66] GAO/AIMD-98-240, September 18, 1998.

[67] Year 2000 Computing Crisis: Action Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/T-AIMD-99-136, April 15, 1999).

Banking and Finance Sector

A large portion of the institutions that make up the banking and finance sector are overseen by one or more federal regulatory agencies. In September 1998 we testified on the efforts of five federal financial regulatory agencies[68] to ensure that the institutions that they oversee are ready to handle the Year 2000 problem.[69] We concluded that the regulators had made significant progress in assessing the readiness of member institutions and in raising awareness on important issues such as contingency planning and testing. Regulator examinations of bank, thrift, and credit union Year 2000 efforts found that the vast majority were doing a satisfactory job of addressing the problem. Nevertheless, the regulators faced the challenge of ensuring that they are ready to take swift action to address those institutions that falter in the later stages of correction and to address disruptions caused by international and public infrastructure failures.

In April, we reported that the Federal Reserve System--which is instrumental to our nation's economic well-being, since it provides depository institutions and government agencies services such as processing checks and transferring funds and securities, has effective controls to help ensure that its Year 2000 progress is reported accurately and reliably.[70] We also found that it is effectively managing the renovation and testing of its internal systems and the development and planned testing of contingency plans for continuity of business operations. Nevertheless, the Federal Reserve System still had much to accomplish before it is fully ready for January 1, 2000, such as completing validation and implementation of all of its internal systems and completing its contingency plans.

In addition to the domestic banking and finance sector, large U.S. financial institutions have financial exposures and relationships with international financial institutions and markets that may be at risk if these international organizations are not ready for the date change occurring on January 1, 2000. In April, we reported[71] that foreign financial institutions had reportedly lagged behind their U.S. counterparts in preparing for the Year 2000 date change. Officials from four of the seven large foreign financial institutions we visited said they had scheduled completion of their Year 2000 preparations about 3 to 6 months after their U.S. counterparts, but they planned to complete their efforts by mid-1999 at the latest. Moreover, key international market supporters, such as those that transmit financial messages and provide clearing and settlement services, told us that

[68] The National Credit Union Administration, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Federal Reserve System, and the Office of the Comptroller of the Currency.

[69] Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain (GAO/T-AIMD-98-305, September 17, 1998).

[70] Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Conversion (GAO/AIMD-99-78, April 9, 1999).

[71] Year 2000: Financial Institution and Regulatory Efforts to Address International Risks (GAO/GGD-99-62, April 27, 1999).

their systems were ready for the date change and that they had begun testing with the financial organizations that depended on these systems. Further, we found that seven large U.S. banks and securities firms we visited were taking actions to address their international risks. In addition, U.S. banking and securities regulators were also addressing the international Year 2000 risks of the institutions that they oversee.

With respect to the insurance industry, in March, we concluded that insurance regulator presence regarding the Year 2000 area was not as strong as that exhibited by the banking and securities industry.[72] State insurance regulators we contacted were late in raising industry awareness of potential Year 2000 problems, provided little guidance to regulated institutions, and failed to convey clear regulatory expectations to companies about Year 2000 preparations and milestones. Nevertheless, the insurance industry is reported by both its regulators and by other outside observers to be generally on track to being ready for 2000. However, most of these reports are based on self-reported information and, compared to other financial regulators, insurance regulators' efforts to validate this information generally began late and were more limited.

In a related report in April,[73] we stated that variations in oversight approaches by state insurance regulators also made it difficult to ascertain the overall status of the insurance industry's Year 2000 readiness. We reported that the magnitude of insurers' Year 2000-related liability exposures could not be estimated at that time but that costs associated with these exposures could be substantial for some property-casualty insurers, particularly those concentrated in commercial-market sectors. In addition, despite efforts to mitigate potential exposures, the Year 2000-related costs that may be incurred by insurers would remain uncertain until key legal issues and actions on pending legislation were resolved.

Transportation Sector

A key component to the nation's transportation sector are airports. This January we reported on our survey of 413 airports.[74] We found that while the nation's airports were making progress in preparing for the year 2000, such progress varied. Of the 334 airports responding to our survey, about one-third reported that they would complete their Year 2000 preparations by June 30, 1999. The other two-thirds either planned on a later date or failed to estimate any completion date, and half of these airports did not have contingency plans for any of 14 core airport functions. Although most of those not expecting to be ready by June 30 are small airports, 26 of them are among the nation's largest 50 airports.

[72] Insurance Industry: Regulators Are Less Active in Encouraging and Validating Year 2000 Preparedness (GAO/T-GGD-99-56, March 11, 1999).

[73] Year 2000: State Insurance Regulators Face Challenges in Determining Industry Readiness (GAO/GGD-99-87, April 30, 1999).

[74] Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem (GAO/RCED/AIMD-99-57, January 29, 1999).

International

In addition to the risks associated with the nation's key economic sectors, one of the largest and most uncertain area of risk relates to the global nature of the problem. Table 3 summarizes the results of the Department of State's Office of the Inspector General's analysis of "Y2K Host Country Infrastructure" assessments submitted by U.S. embassies in 161 countries (98 from the developing world, 24 from former Easter bloc countries and the New Independent States, and 39 from industrialized countries). The following table shows that about half of the countries are reported to be at medium or high risk of having Year 2000-related failures in the key areas of telecommunications, transportation, and energy. While a smaller number of countries were reported at medium or high risk in the finance and water sectors, at least one third of the countries fell into the medium or high risk categories.

Table 3: Risk of Year 2000-Related Sector Failures in 161 Countries

Risk Level	Finance	Telecommunications	Transportation	Energy	Water
High	11	35	18	26	7
Medium	43	56	61	64	52
Low	107	70	82	71	102

Source: Year 2000 Computer Problem: Global Readiness and International Trade (Statement of the Department of State's Inspector General before the Senate Special Committee on the Year 2000 Technology Problem, July 22, 1999).

The Department of State Inspector General concluded that the global community is likely to experience varying degrees of Year 2000-related failures—from mere annoyances to failures in key infrastructure systems—in every sector, region, and economic level. In particular, the Inspector General testified on July 22, 1999, that

- Industrialized countries were generally at low risk of having Year 2000-related infrastructure failures although some of these countries were at risk.
- Developing countries were lagging behind and were struggling to find the financial and technical resources needed to resolve their Year 2000 problems.
- Former Eastern bloc countries were late in getting started and were generally unable to provide detailed information on their Year 2000 programs.

The impact of Year 2000-induced failures in foreign countries could adversely affect the United States, particularly as it relates to the supply chain. To address the international supply chain issue, in January 1999 we suggested[75] that the President's Council on Year

[75] GAO/T-AIMD-99-50, January 20, 1999.

2000 Conversion prioritize trade and commerce activities that are critical to the nation's well-being (e.g., oil, food, pharmaceuticals) and, working with the private sector, identify options for obtaining these materials through alternative avenues in the event that Year 2000-induced failures in the other country or in the transportation sector prevent these items from reaching the United States. In commenting on this suggestion, the Chair stated that the Council had (1) worked with federal agencies to identify sectors with the greatest dependence on international trade, (2) held industry roundtable discussions with the pharmaceutical and food supply sectors, and (3) hosted bilateral and trilateral meetings with the Council's counterparts in Canada and Mexico—the United States' largest trading partners.

- - - - -

In summary, while improvement has been shown, much work remains at the national, federal, state, and local levels to ensure that major service disruptions do not occur. Specifically, remediation must be completed, end-to-end testing performed, and business continuity and contingency plans developed. Similar actions remain to be completed by the nation's key sectors. Accordingly, whether the United States successfully confronts the Year 2000 challenge will largely depend on the success of federal, state, and local governments, as well as the private sector working separately and together to complete these actions. Accordingly, strong leadership and partnerships must be maintained to ensure that the needs of the public are met at the turn of the century.

Mr. Chairman, this concludes my statement. I would be happy to respond to any questions that you or other members of the Subcommittee may have at this time.

Contacts

For information concerning this testimony, please contact Joel Willemssen at (202) 512-6253 or by e-mail at willemssenj.aimd@gao.gov.

Federal High-Impact Programs and Lead Agencies

Agency	Program
Department of Agriculture	Child Nutrition Programs
Department of Agriculture	Food Safety Inspection
Department of Agriculture	Food Stamps
Department of Agriculture	Special Supplemental Nutrition Program for Women, Infants, and Children
Department of Commerce	Patent and trademark processing
Department of Commerce	Weather Service
Department of Defense	Military Hospitals
Department of Defense	Military Retirement
Department of Education	Student Aid
Department of Energy	Federal electric power generation and delivery
Department of Health and Human Services	Child Care
Department of Health and Human Services	Child Support Enforcement
Department of Health and Human Services	Child Welfare
Department of Health and Human Services	Disease monitoring and the ability to issue warnings
Department of Health and Human Services	Indian Health Service
Department of Health and Human Services	Low Income Home Energy Assistance Program
Department of Health and Human Services	Medicaid
Department of Health and Human Services	Medicare
Department of Health and Human Services	Organ Transplants
Department of Health and Human Services	Temporary Assistance for Needy Families
Department of Housing and Urban Development	Housing loans (Government National Mortgage Association)

Department of Housing and Urban Development	Section 8 Rental Assistance
Department of Housing and Urban Development	Public Housing
Department of Housing and Urban Development	FHA Mortgage Insurance
Department of Housing and Urban Development	Community Development Block Grants
Department of the Interior	Bureau of Indians Affairs programs
Department of Justice	Federal Prisons
Department of Justice	Immigration
Department of Justice	National Crime Information Center
Department of Labor	Unemployment Insurance
Department of State	Passport Applications and Processing
Department of Transportation	Air Traffic Control System
Department of Transportation	Maritime Safety Program
Department of the Treasury	Cross-border Inspection Services
Department of Veterans Affairs	Veterans' Benefits
Department of Veterans Affairs	Veterans' Health Care
Federal Emergency Management Agency	Disaster Relief
Office of Personnel Management	Federal Employee Health Benefits
Office of Personnel Management	Federal Employee Life Insurance
Office of Personnel Management	Federal Employee Retirement Benefits
Railroad Retirement Board	Retired Rail Workers Benefits
Social Security Administration	Social Security Benefits
U.S. Postal Service	Mail Service

GAO REPORTS AND TESTIMONY ADDRESSING THE YEAR 2000 CRISIS

Year 2000 Computing Challenge: Agencies' Reporting of Mission-Critical Classified Systems (GAO/AIMD-99-218, August 5, 1999)

Social Security Administration: Update on Year 2000 and Other Key Information Technology Initiatives (GAO/T-AIMD-99-259, July 29, 1999)

Year 2000 Computing Crisis: Status of Medicare Providers Unknown (GAO/AIMD-99-243, July 28, 1999)

Reported Y2K status of the 21 Largest U.S. Cities (GAO/AIMD-99-246R, July 15, 1999)

Year 2000 Computing Challenge: Federal Efforts to Ensure Continued Delivery of Key State-Administered Benefits (GAO/T-AIMD-99-241, July 15, 1999)

Emergency and State and Local Law Enforcement Systems: Committee Questions Concerning Year 2000 Challenges (GAO/AIMD-99-247R, July 14, 1999)

Year 2000 Computing Challenge: Important Progress Made, Yet Much Work Remains to Avoid Disruption of Critical Services (GAO/T-AIMD-99-234, July 9, 1999)

Year 2000 Computing Challenge: Readiness Improving Yet Avoiding Disruption of Critical Services Will Require Additional Work (GAO/T-AIMD-99-233, July 8, 1999)

Year 2000 Computing Challenge: Readiness Improving But Much Work Remains to Avoid Disruption of Critical Services (GAO/T-AIMD-99-232, July 7, 1999)

Defense Computers: Management Controls Are Critical To Effective Year 2000 Testing (GAO/AIMD-99-172, June 30, 1999)

Year 2000 Computing Crisis: Customs is Making Good Progress (GAO/T-AIMD-99-225, June 29, 1999)

Year 2000 Computing Challenge: Delivery of Key Benefits Hinges on States' Achieving Compliance (GAO/T-AIMD/GGD-99-221, June 23, 1999)

Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications (GAO/T-AIMD-99-214, June 22, 1999).

GSA's Effort to Develop Year 2000 Business Continuity and Contingency Plans for Telecommunications Systems (GAO/AIMD-99-201R, June 16, 1999).

Year 2000 Computing Crisis: Actions Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/AIMD-99-190R, June 11, 1999)

Year 2000 Computing Challenge: Concerns About Compliance Information on Biomedical Equipment (GAO/T-AIMD-99-209, June 10, 1999)

Year 2000 Computing Challenge: Much Biomedical Equipment Status Information Available, Yet Concerns Remain (GAO/T-AIMD-99-197, May 25, 1999)

Year 2000 Computing Challenge: OPM Has Made Progress on Business Continuity Planning (GAO/GGD-99-66, May 24, 1999)

VA Y2K Challenges: Responses to Post-Testimony Questions (GAO/AIMD-99-199R, May 24, 1999)

Year 2000 Computing Crisis: USDA Needs to Accelerate Time Frames for Completing Contingency Planning (GAO/AIMD-99-178, May 21, 1999)

Year 2000 Computing Crisis: Readiness of the Oil and Gas Industries (GAO/AIMD-99-162, May 19, 1999)

Year 2000 Computing Challenge: Time Issues Affecting the Global Positioning System (GAO/T-AIMD-99-187, May 12, 1999)

Year 2000 Computing Challenge: Education Taking Needed Actions But Work Remains (GAO/T-AIMD-99-180, May 12, 1999)

Year 2000 Computing Challenge: Labor Has Progressed But Selected Systems Remain at Risk (GAO/T-AIMD-99-179, May 12, 1999)

Year 2000: State Insurance Regulators Face Challenges in Determining Industry Readiness (GAO/GGD-99-87, April 30, 1999)

Year 2000 Computing Challenge: Status of Emergency and State and Local Law Enforcement Systems Is Still Unknown (GAO/T-AIMD-99-163, April 29, 1999)

Year 2000 Computing Crisis: Costs and Planned Use of Emergency Funds (GAO/AIMD-99-154, April 28, 1999)

Year 2000: Financial Institution and Regulatory Efforts to Address International Risks (GAO/GGD-99-62, April 27, 1999)

Year 2000 Computing Crisis: Readiness of Medicare and the Health Care Sector (GAO/T-AIMD-99-160, April 27, 1999)

U.S. Postal Service: Subcommittee Questions Concerning Year 2000 Challenges Facing the Service (GAO/AIMD-99-150R, April 23, 1999)

Year 2000 Computing Crisis: Status of the Water Industry (GAO/AIMD-99-151, April 21, 1999)

Year 2000 Computing Crisis: Key Actions Remain to Ensure Delivery of Veterans Benefits and Health Services (GAO/T-AIMD-99-152, April 20, 1999)

Year 2000 Computing Crisis: Readiness Improving But Much Work Remains To Ensure Delivery of Critical Services (GAO/T-AIMD-99-149, April 19, 1999)

Year 2000 Computing Crisis: Action Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/T-AIMD-99-136, April 15, 1999)

Year 2000 Computing Challenge: Federal Government Making Progress But Critical Issues Must Still Be Addressed to Minimize Disruptions (GAO/T-AIMD-99-144, April 14, 1999)

Year 2000 Computing Crisis: Additional Work Remains to Ensure Delivery of Critical Services (GAO/T-AIMD-99-143, April 13, 1999)

Tax Administration: IRS' Fiscal Year 2000 Budget Request and 1999 Tax Filing Season (GAO/T-GGD/AIMD-99-140, April 13, 1999).

Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Conversion (GAO/AIMD-99-78, April 9, 1999)

Year 2000 Computing Crisis: Readiness of the Electric Power Industry (GAO/AIMD-99-114, April 6, 1999)

Year 2000 Computing Crisis: Customs Has Established Effective Year 2000 Program Controls (GAO/AIMD-99-37, March 29, 1999)

Year 2000 Computing Crisis: FAA Is Making Progress But Important Challenges Remain (GAO/T-AIMD/RCED-99-118, March 15, 1999)

Insurance Industry: Regulators Are Less Active in Encouraging and Validating Year 2000 Preparedness (GAO/T-GGD-99-56, March 11, 1999)

Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed (GAO/T-AIMD-99-101, March 2, 1999)

Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services (GAO/T-AIMD-99-92, February 26, 1999)

Defense Information Management: Continuing Implementation Challenges Highlight the Need for Improvement (GAO/T-AIMD-99-93, February 25, 1999)

IRS' Year 2000 Efforts: Status and Remaining Challenges (GAO/T-GGD-99-35, February 24, 1999)

Department of Commerce: National Weather Service Modernization and NOAA Fleet Issues (GAO/T-AIMD/GGD-99-97, February 24, 1999)

Year 2000 Computing Crisis: Medicare and the Delivery of Health Services Are at Risk (GAO/T-AIMD-99-89, February 24, 1999)

Year 2000 Computing Crisis: Readiness of State Automated Systems That Support Federal Human Services Programs (GAO/T-AIMD-99-91, February 24, 1999)

Year 2000 Computing Crisis: Customs Is Effectively Managing Its Year 2000 Program (GAO/T-AIMD-99-85, February 24, 1999)

Year 2000 Computing Crisis: Update on the Readiness of the Social Security Administration (GAO/T-AIMD-99-90, February 24, 1999)

Year 2000 Computing Crisis: Challenges Still Facing the U.S. Postal Service (GAO/T-AIMD-99-86, February 23, 1999)

Year 2000 Computing Crisis: The District of Columbia Remains Behind Schedule (GAO/T-AIMD-99-84, February 19, 1999)

High-Risk Series: An Update (GAO/HR-99-1, January 1999)

Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem (GAO/RCED/AIMD-99-57, January 29, 1999)

Defense Computers: DOD's Plan for Execution of Simulated Year 2000 Exercises (GAO/AIMD-99-52R, January 29, 1999)

Year 2000 Computing Crisis: Status of Bureau of Prisons' Year 2000 Efforts (GAO/AIMD-99-23, January 27, 1999)

Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, January 20, 1999)

Year 2000 Computing Challenge: Readiness Improving, But Critical Risks Remain (GAO/T-AIMD-99-49, January 20, 1999)

Status Information: FAA's Year 2000 Business Continuity and Contingency Planning Efforts Are Ongoing (GAO/AIMD-99-40R, December 4, 1998)

Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, November 1998)

Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998)

Year 2000 Computing Crisis: Status of Efforts to Deal With Personnel Issues (GAO/AIMD/GGD-99-14, October 22, 1998)

Year 2000 Computing Crisis: Updated Status of Department of Education's Information Systems (GAO/T-AIMD-99-8, October 8, 1998)

Year 2000 Computing Crisis: The District of Columbia Faces Tremendous Challenges in Ensuring That Vital Services Are Not Disrupted (GAO/T-AIMD-99-4, October 2, 1998)

Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy (GAO/AIMD-98-284, September 28, 1998)

Year 2000 Computing Crisis: Leadership Needed to Collect and Disseminate Critical Biomedical Equipment Information (GAO/T-AIMD-98-310, September 24, 1998)

Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown (GAO/AIMD-98-240, September 18, 1998)

Year 2000 Computing Crisis: Significant Risks Remain to Department of Education's Student Financial Aid Systems (GAO/T-AIMD-98-302, September 17, 1998)

Year 2000 Computing Crisis: Progress Made at Department of Labor, But Key Systems at Risk (GAO/T-AIMD-98-303, September 17, 1998)

Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain (GAO/T-AIMD-98-305, September 17, 1998)

Year 2000 Computing Crisis: Federal Reserve Is Acting to Ensure Financial Institutions Are Fixing Systems But Challenges Remain (GAO/AIMD-98-248, September 17, 1998)

Responses to Questions on FAA's Computer Security and Year 2000 Program (GAO/AIMD-98-301R, September 14, 1998)

Year 2000 Computing Crisis: Severity of Problem Calls for Strong Leadership and Effective Partnerships (GAO/T-AIMD-98-278, September 3, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Partnerships Needed to Reduce Likelihood of Adverse Impact (GAO/T-AIMD-98-277, September 2, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Partnerships Needed to Mitigate Risks (GAO/T-AIMD-98-276, September 1, 1998)

Year 2000 Computing Crisis: State Department Needs To Make Fundamental Improvements To Its Year 2000 Program (GAO/AIMD-98-162, August 28, 1998)

Year 2000 Computing: EFT 99 Is Not Expected to Affect Year 2000 Remediation Efforts (GAO/AIMD-98-272R, August 28, 1998)

Year 2000 Computing Crisis: Progress Made in Compliance of VA Systems, But Concerns Remain (GAO/AIMD-98-237, August 21, 1998)

Year 2000 Computing Crisis: Avoiding Major Disruptions Will Require Strong Leadership and Effective Partnerships (GAO/T-AIMD-98-267, August 19, 1998)

Year 2000 Computing Crisis: Strong Leadership and Partnerships Needed to Address Risk of Major Disruptions (GAO/T-AIMD-98-266, August 17, 1998)

Year 2000 Computing Crisis: Strong Leadership and Partnerships Needed to Mitigate Risk of Major Disruptions (GAO/T-AIMD-98-262, August 13, 1998)

FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998)

Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, August 1998)

Internal Revenue Service: Impact of the IRS Restructuring and Reform Act on Year 2000 Efforts (GAO/GGD-98-158R, August 4, 1998)

Social Security Administration: Subcommittee Questions Concerning Information Technology Challenges Facing the Commissioner (GAO/AIMD-98-235R, July 10, 1998)

Year 2000 Computing Crisis: Actions Needed on Electronic Data Exchanges (GAO/AIMD-98-124, July 1, 1998)

Defense Computers: Year 2000 Computer Problems Put Navy Operations At Risk (GAO/AIMD-98-150, June 30, 1998)

Year 2000 Computing Crisis: Testing and Other Challenges Confronting Federal Agencies (GAO/T-AIMD-98-218, June 22, 1998)

Year 2000 Computing Crisis: Telecommunications Readiness Critical, Yet Overall Status Largely Unknown (GAO/T-AIMD-98-212, June 16, 1998)

GAO Views on Year 2000 Testing Metrics (GAO/AIMD-98-217R, June 16, 1998)

IRS' Year 2000 Efforts: Business Continuity Planning Needed for Potential Year 2000 System Failures (GAO/GGD-98-138, June 15, 1998)

Year 2000 Computing Crisis: Actions Must Be Taken Now to Address Slow Pace of Federal Progress (GAO/T-AIMD-98-205, June 10, 1998)

Defense Computers: Army Needs to Greatly Strengthen Its Year 2000 Program (GAO/AIMD-98-53, May 29, 1998)

Year 2000 Computing Crisis: USDA Faces Tremendous Challenges in Ensuring That Vital Public Services Are Not Disrupted (GAO/T-AIMD-98-167, May 14, 1998)

Securities Pricing: Actions Needed for Conversion to Decimals (GAO/T-GGD-98-121, May 8, 1998)

Year 2000 Computing Crisis: Continuing Risks of Disruption to Social Security, Medicare, and Treasury Programs (GAO/T-AIMD-98-161, May 7, 1998)

IRS' Year 2000 Efforts: Status and Risks (GAO/T-GGD-98-123, May 7, 1998)

Air Traffic Control: FAA Plans to Replace Its Host Computer System Because Future Availability Cannot Be Assured (GAO/AIMD-98-138R, May 1, 1998)

Year 2000 Computing Crisis: Potential For Widespread Disruption Calls For Strong Leadership and Partnerships (GAO/AIMD-98-85, April 30, 1998)

Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998)

Department of the Interior: Year 2000 Computing Crisis Presents Risk of Disruption to Key Operations (GAO/T-AIMD-98-149, April 22, 1998)

Tax Administration: IRS' Fiscal Year 1999 Budget Request and Fiscal Year 1998 Filing Season (GAO/T-GGD/AIMD-98-114, March 31, 1998)

Year 2000 Computing Crisis: Strong Leadership Needed to Avoid Disruption of Essential Services (GAO/T-AIMD-98-117, March 24, 1998)

Year 2000 Computing Crisis: Federal Regulatory Efforts to Ensure Financial Institution Systems Are Year 2000 Compliant (GAO/T-AIMD-98-116, March 24, 1998)

Year 2000 Computing Crisis: Office of Thrift Supervision's Efforts to Ensure Thrift Systems Are Year 2000 Compliant (GAO/T-AIMD-98-102, March 18, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Public/Private Cooperation Needed to Avoid Major Disruptions (GAO/T-AIMD-98-101, March 18, 1998)

Post-Hearing Questions on the Federal Deposit Insurance Corporation's Year 2000 (Y2K) Preparedness (AIMD-98-108R, March 18, 1998)

SEC Year 2000 Report: Future Reports Could Provide More Detailed Information (GAO/GGD/AIMD-98-51, March 6, 1998)

Year 2000 Readiness: NRC's Proposed Approach Regarding Nuclear Powerplants (GAO/AIMD-98-90R, March 6, 1998)

Year 2000 Computing Crisis: Federal Deposit Insurance Corporation's Efforts to Ensure Bank Systems Are Year 2000 Compliant (GAO/T-AIMD-98-73, February 10, 1998)

Year 2000 Computing Crisis: FAA Must Act Quickly to Prevent Systems Failures (GAO/T-AIMD-98-63, February 4, 1998)

FAA Computer Systems: Limited Progress on Year 2000 Issue Increases Risk Dramatically (GAO/AIMD-98-45, January 30, 1998)

Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998)

Year 2000 Computing Crisis: Actions Needed to Address Credit Union Systems' Year 2000 Problem (GAO/AIMD-98-48, January 7, 1998)

Veterans Health Administration Facility Systems: Some Progress Made In Ensuring Year 2000 Compliance, But Challenges Remain (GAO/AIMD-98-31R, November 7, 1997)

Year 2000 Computing Crisis: National Credit Union Administration's Efforts to Ensure Credit Union Systems Are Year 2000 Compliant (GAO/T-AIMD-98-20, October 22, 1997)

Social Security Administration: Significant Progress Made in Year 2000 Effort, But Key Risks Remain (GAO/AIMD-98-6, October 22, 1997)

Defense Computers: Technical Support Is Key to Naval Supply Year 2000 Success (GAO/AIMD-98-7R, October 21, 1997)

Defense Computers: LSSC Needs to Confront Significant Year 2000 Issues (GAO/AIMD-97-149, September 26, 1997)

Veterans Affairs Computer Systems: Action Underway Yet Much Work Remains To Resolve Year 2000 Crisis (GAO/T-AIMD-97-174, September 25, 1997)

Year 2000 Computing Crisis: Success Depends Upon Strong Management and Structured Approach, (GAO/T-AIMD-97-173, September 25, 1997)

Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997)

Defense Computers: SSG Needs to Sustain Year 2000 Progress (GAO/AIMD-97-120R, August 19, 1997)

Defense Computers: Improvements to DOD Systems Inventory Needed for Year 2000 Effort (GAO/AIMD-97-112, August 13, 1997)

Defense Computers: Issues Confronting DLA in Addressing Year 2000 Problems (GAO/AIMD-97-106, August 12, 1997)

Defense Computers: DFAS Faces Challenges in Solving the Year 2000 Problem (GAO/AIMD-97-117, August 11, 1997)

Year 2000 Computing Crisis: Time is Running Out for Federal Agencies to Prepare for the New Millennium (GAO/T-AIMD-97-129, July 10, 1997)

Veterans Benefits Computer Systems: Uninterrupted Delivery of Benefits Depends on Timely Correction of Year-2000 Problems (GAO/T-AIMD-97-114, June 26, 1997)

Veterans Benefits Computer Systems: Risks of VBA's Year-2000 Efforts (GAO/AIMD-97-79, May 30, 1997)

Medicare Transaction System: Success Depends Upon Correcting Critical Managerial and Technical Weaknesses (GAO/AIMD-97-78, May 16, 1997)

Medicare Transaction System: Serious Managerial and Technical Weaknesses Threaten Modernization (GAO/T-AIMD-97-91, May 16, 1997)

Year 2000 Computing Crisis: Risk of Serious Disruption to Essential Government Functions Calls for Agency Action Now (GAO/T-AIMD-97-52, February 27, 1997)

Year 2000 Computing Crisis: Strong Leadership Today Needed To Prevent Future Disruption of Government Services (GAO/T-AIMD-97-51, February 24, 1997)

High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997)

(511788)

Mr. HORN. Our next witness is Mark Burton, the Y2K project manager for the city of San Jose, and, Mark, we're delighted with the kindness of the city administration to let us use their City Council Chamber today. So we thank you.

Mr. BURTON. Thank you. Good morning. Thank you for opportunity to speak before the subcommittee on the city of San Jose's efforts in preparing for a rollover in the millennium and how we're addressing the year 2000 computer problem.

The city began its year 2000 efforts in the summer of 1997, and since that time has allocated over $10 million toward this effort, with $6 million of that at our airport alone to mitigate the impacts of Y2K computer interruptions.

The Y2K Office in the Information Technology Department has had the responsibility for coordination of planning and remediation activities for Y2K efforts. In addition, the Information Technology Department has responsibility for the mitigation and year 2000 readiness for the city's traditional computer systems. Individual departments have focused on their internal systems and operational issues, and the Y2K task force comprised of representatives from all departments have focused on coordination activities between the departments and acted as a clearing house for Y2K information.

In early 1999, recognizing the potential impacts of service interruptions on our critical health and safety services, a second Y2K Public Health and Safety Task Force was created to concentrate on the readiness for these services. This Public Health and Safety Task Force's focus is on emergency and health issues. Some examples include water service, waste water treatment, emergency medical response, emergency police response, sewage collection and storm drainage.

Our year 2000 project has four major areas: Computer systems, embedded systems chips, business continuity planning and public information. In the computer systems area, systems and hardware were inventoried and assessed for operation into and through the year 2000. We inventoried and assessed over 160 systems and 150 applications for computers and servers. After Y2K assessment, decisions were made to repair, upgrade, replace or retire in-house and vendor supplied software. 15 systems remain in the remediation process at this time.

For embedded systems chips, in critical service areas including our Convention Center, police and fire departments, municipal water service, telecommunications and streets, the city obtained services of expert contractors in embedded chips to assist in the inventory assessment. In these six departments, 2,500 pieces of equipment were inventoried and assessed. While the majority of the equipment was found to be year 2000 compliant in the assessment phase, over 30 percent was found questionable, and just over 1 percent not Y2K compliant.

While interesting to find embedded systems chips in equipment, appliances and other things taken for granted both at home and work, it was surprising to find non-year 2000 compliant chips in our fire department's defibrillators. They are now year 2000 compliant, and Deputy Chief McMillan will go into more detail about the defibrillators.

In late 1998 the city began its business continuing planning with development of department Y2K contingency strategies for mission critical and essential services and equipment. Preliminary plans were developed between December 1998 and March 1999 with more comprehensive plans recently completed in July. We are not only preparing the computer systems for the date change, we are also preparing contingency strategies which will be implemented, if required, to minimize disruptions of critical services. In the case of a temporary or more extended service interruption, we must be prepared with recovery strategies to bridge the gap and continue supplying critical services.

With our dependency on others for services and products in our complex industrial technological society, we are taking the steps to ensure the continuation of critical city services should there be interruptions. Staff has developed detailed contingency plans for all critical services and systems. These contingency plans are based on our existing emergency operations plan, and they detail the procedures necessary to mitigate service impacts related to year 2000 failures, either locally, or in the event of power-grid outages or utility systems malfunctions. Dr. Winslow's testimony covers some of the training and practice exercises used to prepare staff and tune our contingency plans.

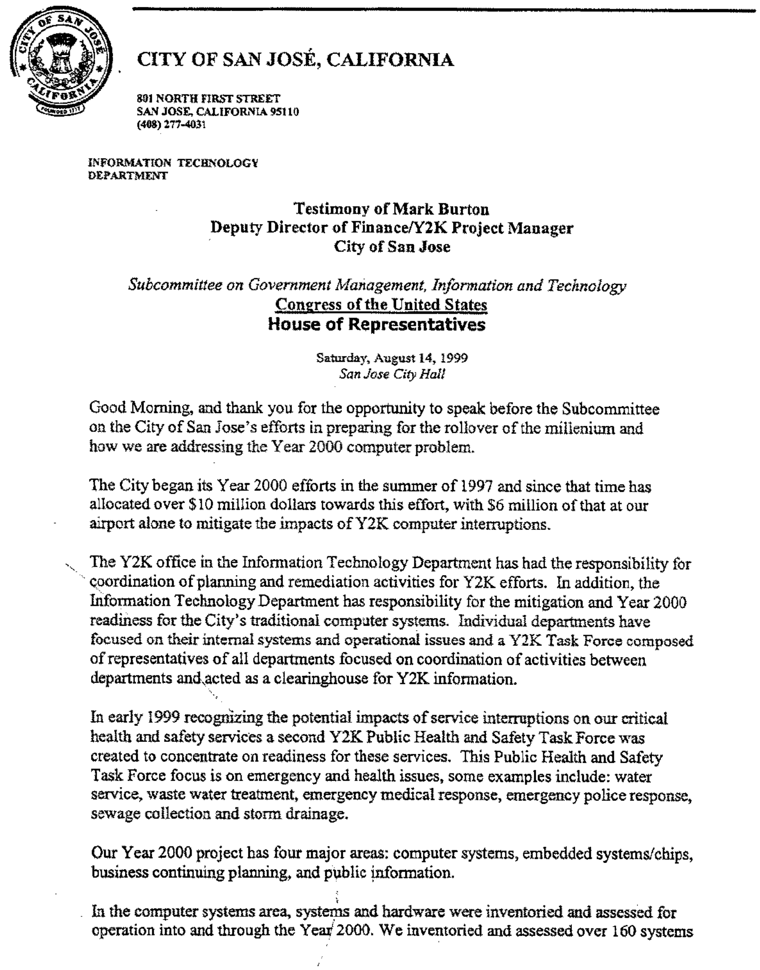
The last component of our Y2K project I want to speak of is the public information phase. The city with the assistance of a media consultant is in the process of developing a public outreach campaign to reach out to residents to assist them with year 2000 home readiness. We're coordinating this with Santa Clara County and targeting our initial release for October to coincide with the 10th anniversary of the Loma Prieta earthquake. The emphasis will be on emergency preparedness, not only for year 2000, but for any emergency, be it earthquake or other natural disaster. Another area of concentration will be to educate city employees in home preparedness so they will be ready to respond to any Y2K problems with the knowledge that their families are OK.

The city of San Jose has made good progress on its systems readiness for Y2K. However, due to our reliance on others for key services and supplies, the city is taking steps to be ready for Y2K interruptions whether they come from within or from a third party. The city's goal is clear, to be prepared for Y2K. Mission-critical systems and services must be ready for the new millennium, and at this time we see no reason that the city should not meet this goal.

In conclusion, I'd like to thank the committee for the time to speak on the city of San Jose's year 2000 efforts.

Mr. HORN. Well, thank you very much for your well-organized description of what you've gone through and what some of the implications are, and we'll get back to some of this in the question period.

[The prepared statement of Mr. Burton follows:]



CITY OF SAN JOSÉ, CALIFORNIA

801 NORTH FIRST STREET
SAN JOSE, CALIFORNIA 95110
(408) 277-4031

INFORMATION TECHNOLOGY
DEPARTMENT

Testimony of Mark Burton
Deputy Director of Finance/Y2K Project Manager
City of San Jose

Subcommittee on Government Management, Information and Technology
Congress of the United States
House of Representatives

Saturday, August 14, 1999
San Jose City Hall

Good Morning, and thank you for the opportunity to speak before the Subcommittee on the City of San Jose's efforts in preparing for the rollover of the millenium and how we are addressing the Year 2000 computer problem.

The City began its Year 2000 efforts in the summer of 1997 and since that time has allocated over $10 million dollars towards this effort, with $6 million of that at our airport alone to mitigate the impacts of Y2K computer interruptions.

The Y2K office in the Information Technology Department has had the responsibility for coordination of planning and remediation activities for Y2K efforts. In addition, the Information Technology Department has responsibility for the mitigation and Year 2000 readiness for the City's traditional computer systems. Individual departments have focused on their internal systems and operational issues and a Y2K Task Force composed of representatives of all departments focused on coordination of activities between departments and acted as a clearinghouse for Y2K information.

In early 1999 recognizing the potential impacts of service interruptions on our critical health and safety services a second Y2K Public Health and Safety Task Force was created to concentrate on readiness for these services. This Public Health and Safety Task Force focus is on emergency and health issues, some examples include: water service, waste water treatment, emergency medical response, emergency police response, sewage collection and storm drainage.

Our Year 2000 project has four major areas: computer systems, embedded systems/chips, business continuing planning, and public information.

In the computer systems area, systems and hardware were inventoried and assessed for operation into and through the Year 2000. We inventoried and assessed over 160 systems be to educate City employees in home preparedness so they will be ready to respond to any Y2K problems with the knowledge that their families are OK.

The City of San Jose has made good progress on it's systems readiness for Year 2000. However, due to our reliance on others for key services and supplies the City is taking steps to be ready for Y2K interruptions whether they come from within or from a third party. The City's goal is clear to be prepared for Y2K. Mission critical systems and services must be ready for the new millenium and at this time we see no reason that the City should not meet this goal.

In conclusion, I'd like to thank the committee for the time to speak on the City of San Jose's Year 2000 efforts.

Mr. HORN. Dana Drysdale is the vice president, information systems for the San Jose Water Co.

Mr. DRYSDALE. Thank you, Chairman Horn. In the interest of time, I will skip our greeting and summary that's in the written statement and go directly to some detail which will be of use to you. We're very pleased to be here today. In my testimony, San Jose Water Co. will be referred to as SJWC.

SJWC's Y2K readiness program can be summarized into six major steps. These steps are: No. 1. Customer contact. Every customer that requests information regarding San Jose Water Co.'s Y2K readiness program receives a personal written reply. Additionally, there is Y2K information on sjwater.com. That's our website.

Step 2. Major power and water supplier contact. Both Pacific Gas and Electric Co. and the Santa Clara Valley Water District are critical to the normal operation of Silicon Valley's water system. These organizations have a Y2K readiness program. SJWC and all local water retailers meet quarterly as a group with the Water District. The April 21, 1999 meeting was devoted to a discussion of Y2K.

The district shares knowledge of State and Federal water project readiness levels. As of June 1999, SJWC understands that the State completed the modification to its network to be Y2K ready and that these modifications are being tested by a consultant. As a result of the April 21st meeting, the district and SJWC identified a continuous supply of electrical power as a concern. Additional information about this is included in Step 6, contingency planning.

Step 3 of our program. Review of software and hardware products. SJWC uses standard commercially available computer hardware and software packages. This means we do not have a significant development environment at the San Jose Water Co. All SJWC hardware and software suppliers perform significant Y2K testing of their products. In many cases, these software and hardware providers also engage independent testing organizations, such as ITAA or NSTL. To the best of our knowledge, all software and hardware products used in SJWC's water system are Y2K ready.

Where practical, SJWC repeated aspects of these tests. For example, water distribution for most of Silicon Valley is controlled by SJWC's sophisticated SCADA System. SJWC performed a successful Y2K system test of the SCADA System's servers and remote telemetry unit's hardware and software.

Step 4. Contacts with governments, other suppliers and business partners. All replies from these folks indicate a Y2K readiness program.

Step 5 of the program. Employee awareness and education. SJWC's executive committee regularly discusses the Y2K readiness program. SJWC's chief financial officer, controller, and vice president of information systems—that's three different people—participated in a Y2K test of SJWC financial and materials systems.

The company's technology committee meets quarterly or as needed to ensure that SJWC uses technology appropriately. The technology committee is also involved in Y2K readiness. For example, this committee has an "embedded controller" project. Committee members identified functions in their area that might be subject to control of a computerized clock and contacted the manufacturer to ensure Y2K readiness. Please note that SJWC's water-related computer systems typically manage water based on demand and not time.

Step 6 of the program. Contingency planning. The chief contingency planning concerns for Silicon Valley's water supply include the import water and electrical power concerns identified in step 2 above. SJWC contingency plans are common for many possible situations in Silicon Valley, including earthquakes.

Water resources in the valley are managed under an integrated plan by Government Agencies, by the Water District and by water suppliers such as SJWC. 50 percent of our water is imported from State and Federal water projects, and is treated at District treatment plants.

Approximately 35 percent and 15 percent, respectively, of Silicon Valley's water is supplied by SJWC operated wells or through local surface water. Local surface water depends on local rainfall. In the event of a disaster or emergency that impacts ground water supplies—excuse me—import water supplies, significant additional ground water is available from SJWC operated wells.

SJWC has excellent working relationships with Pacific Gas and Electric Co. and other power suppliers. In the event of power interruptions, SJWC's experience is that power is restored as quickly as possible. SJWC also has emergency generation facilities that operate the water system during power interruptions such as those experienced during the 1989 Loma Prieta earthquake. However, sustained regional power outages have serious impacts on water operations.

The SJWC portion of Silicon Valley's water system is designed with local finished water storage reservoirs. This means that water is in the valley. In many cases, full local reservoirs and tanks will gravity feed water to customers. Power is needed to initially fill these reservoirs.

On the morning of a typical January day, SJWC will have approximately 2 days of finished water in Silicon Valley in these reservoirs. If power is completely interrupted for more than 2 days, water would be supplied using SJWC emergency facilities alone. Operating the water system under emergency conditions during a sustained regional power outage is very different than typical water delivery, this is beyond that first couple days, and may result in some water supply outages.

Disaster planning and generation facilities are coordinated with county and city agencies and the California Public Utilities Commission. SJWC customers and employees enjoy many benefits from participating in regional emergency preparedness and encourage everyone to take advantage of their city and county emergency planning services.

San Jose Water Co. thanks Chairman Horn and House staff for the opportunity to present testimony. Additional information is available at sjwater.com or by phone at (408) 279–7900.

Mr. HORN. Thank you. That's a very thorough presentation, and you're talking about a key ingredient for all of us. We don't last too long without water. Thank you for coming with that.

[The prepared statement of Mr. Drysdale follows:]

Testimony before the United States House of Representatives Subcommittee on Government Management, Information and Technology by the San Jose Water Company
Field Hearing re: Year 2000 Computer Technology Preparedness
San Jose, California City Council Chambers
August 14, 1999

HONORED CHAIRMAN HORN, REPRESENTATIVE POMBO, DISTINGUISHED MEMBERS OF OUR FEDERAL, STATE AND LOCAL GOVERNMENT, MEDIA AND ALL CITIZENS, SAN JOSE WATER COMPANY IS PLEASED TO HAVE THE OPPORTUNITY TO REPORT ON YEAR 2000 PREPAREDNESS.

THIS TESTIMONY IS LIMITED TO A BRIEF OVERVIEW OF SAN JOSE WATER COMPANY'S Y2K READINESS PROGRAM.

SAN JOSE WATER COMPANY'S Y2K READINESS PROGRAM CAN BE SUMMARIZED INTO SIX MAJOR STEPS. THESE STEPS ARE:

1. CUSTOMER CONTACT. EVERY CUSTOMER THAT REQUESTS INFORMATION REGARDING SAN JOSE WATER COMPANY'S Y2K READINESS PROGRAM RECEIVES A PERSONAL WRITTEN REPLY. ADDITIONALLY, THERE IS Y2K INFORMATION ON SJWATER.COM.
2. CONTACT WITH THE POWER AND WATER SUPPLY CHAIN, SUCH AS THE PACIFIC GAS AND ELECTRIC COMPANY AND THE SANTA CLARA VALLEY WATER DISTRICT.
3. REVIEW OF SOFTWARE AND HARDWARE PRODUCTS.
4. CONTACTS WITH GOVERNMENT ORGANIZATIONS, OTHER SUPPLIERS OF GOODS AND SERVICES AND OTHER BUSINESS PARTNERS.
5. EMPLOYEE AWARENESS AND EDUCATION.
6. CONTINGENCY PLANNING.

WE WILL PRESENT A SMALL AMOUNT OF ADDITIONAL DETAIL REGARDING STEPS 2 - 6 IN THE TIME AVAILABLE. SAN JOSE WATER COMPANY WILL BE REFERRED TO AS SJWC.

2. MAJOR POWER AND WATER SUPPLIERS. BOTH PACIFIC GAS AND ELECTRIC AND THE SANTA CLARA VALLEY WATER DISTRICT ARE CRITICAL TO THE NORMAL OPERATION OF SILICON VALLEY'S WATER SYSTEM. THESE ORGANIZATIONS HAVE A Y2K READINESS PROGRAM. SJWC AND ALL LOCAL WATER RETAILERS MEET QUARTERLY AS A GROUP WITH THE WATER DISTRICT. THE APRIL 21, 1999 MEETING WAS DEVOTED TO A DISCUSSION OF Y2K.

   THE DISTRICT SHARES KNOWLEDGE OF STATE AND FEDERAL WATER PROJECT READINESS LEVELS. AS OF JUNE 1999, SJWC UNDERSTANDS THAT THE STATE COMPLETED THE MODIFICATION TO ITS NETWORK TO BE Y2K READY AND THAT THESE MODIFICATIONS ARE BEING TESTED BY A CONSULTANT. AS A RESULT OF THE APRIL 21 MEETING, THE DISTRICT AND SJWC IDENTIFIED A CONTINUOUS SUPPLY OF

Testimony before the United States House of Representatives
Subcommittee on Government Management, Information and
Technology by the San Jose Water Company
Field Hearing re: Year 2000 Computer Technology Preparedness
San Jose, California City Council Chambers
August 14, 1999

6. CONTINGENCY PLANNING. THE CHIEF CONTINGENCY PLANNING CONCERNS FOR SILICON VALLEY'S WATER SUPPLY INCLUDE THE IMPORT WATER AND ELECTRICAL POWER CONCERNS IDENTIFIED IN ITEM 2., ABOVE. SJWC CONTINGENCY PLANS ARE COMMON TO MANY POSSIBLE SITUATIONS IN SILICON VALLEY, INCLUDING EARTHQUAKE.

   WATER RESOURCES ARE MANAGED UNDER AN INTEGRATED PLAN BY GOVERNMENT AGENCIES, BY THE WATER DISTRICT AND BY WATER SUPPLIERS, SUCH AS SJWC. 50% OF OUR WATER IS IMPORTED FROM STATE AND FEDERAL WATER PROJECTS, AND IS TREATED AT DISTRICT TREATMENT PLANTS.

   APPROXIMATELY 35% AND 15%, RESPECTIVELY, OF SILICON VALLEY'S WATER IS SUPPLIED BY SJWC OPERATED WELLS OR LOCAL SURFACE WATER. LOCAL SURFACE WATER DEPENDS UPON LOCAL RAINFALL. IN THE EVENT OF A DISASTER OR EMERGENCY THAT IMPACTS IMPORT WATER SUPPLIES, SIGNIFICANT ADDITIONAL GROUNDWATER IS AVAILABLE FROM SJWC OPERATED WELLS.

   SJWC HAS EXCELLENT WORKING RELATIONSHIPS WITH PACIFIC GAS AND ELECTRIC COMPANY AND OTHER POWER SUPPLIERS. IN THE EVENT OF POWER INTERRUPTIONS, SJWC'S EXPERIENCE IS THAT POWER IS RESTORED AS QUICKLY AS POSSIBLE. SJWC ALSO HAS EMERGENCY GENERATION FACILITIES THAT OPERATE THE WATER SYSTEM DURING POWER INTERRUPTIONS SUCH AS THOSE EXPERIENCED DURING THE 1989 LOMA PRIETA EARTHQUAKE.

   SUSTAINED REGIONAL POWER OUTAGES HAVE SERIOUS IMPACTS ON WATER OPERATIONS.

   THE SJWC PORTION OF SILICON VALLEY'S WATER SYSTEM IS DESIGNED WITH LOCAL FINISHED WATER STORAGE RESERVOIRS. IN MANY CASES, FULL LOCAL RESERVOIRS AND TANKS WILL GRAVITY FEED WATER TO CUSTOMERS. POWER IS NEEDED TO INITIALLY FILL THE RESERVOIRS.

   ON THE MORNING OF A TYPICAL JANUARY DAY, SJWC WILL HAVE APPROXIMATELY 2 DAYS OF FINISHED WATER IN SILICON VALLEY IN THESE RESERVOIRS. IF POWER IS COMPLETELY INTERRUPTED FOR

Mr. HORN. The next witness is Ronald E. Garratt, assistant city manager for the city of Santa Clara. Mr. Garratt.

Mr. GARRATT. Thank you, Mr. Chairman. I thank you for inviting me to speak today on the subject of Y2K readiness in the city of Santa Clara. I'm both the assistant city manager and year 2000 project manager for the city.

Before I describe the city's Y2K readiness program, I would like to briefly acquaint you with the city of Santa Clara. Santa Clara is a full-service municipality providing police, fire and utility services to approximately 103,000 residents and over 10,000 businesses. Somewhat unique to Santa Clara, we are one of only four cities in the greater Bay Area that own and operate an electric utility. Later on this morning you will be hearing from Karen Lopez, Silicon Valley Power's Y2K program manager.

The city of Santa Clara is either headquarters for or services a major campus site for a number of leading internationally known high-tech companies: Intel, Sun Microsystems, Hewlett Packard, 3Com, Applied Materials and National Semiconductor to name a few.

Like other organizations, the city of Santa Clara knows the importance of year 2000 readiness, and is focused on our ability to store and manage data through the millennium change and into the next century. The city's formal year 2000 program began in 1997. However, the city's actual remediation efforts commenced approximately 5 years ago through the systematic replacement of major departmental computer systems. In point of fact, replacement of the city's then existing mainframe driven COBOL based operating programs were driven as much or more by the need for increased performance and enhanced user functionality as the need to eliminate the expression of a year in a two-digit field.

Over the past 5 years, the city has spent nearly $22 million replacing critical computer systems. $7½ million in public safety systems, including the new 911 emergency dispatch system, the new 800 MHz trunked radio system, new police and fire records management systems and telephone system upgrades. $5½ million for utility systems including the electric substation telemetry control, power scheduling and water system pump control upgrades. $5 million for finance systems including a new utility building system and a finance system data warehouse. $2 million for computer network improvements including the upgrade to Y2K compatible personal computers for all system users, and the upgrade of all network hardware and software to Y2K compatible standards. $1 million for public works systems including the upgrade of the city's traffic control system.

The city is working aggressively toward being a Y2K ready organization for all major systems no later than September 1999 with the exception of two departmental computer systems that will be fully operational by November 1999.

The city's Y2K readiness focuses on two major strategies: Replace or repair. As I mentioned earlier, it has been the city's primary goal to replace non-Y2K compatible systems rather than repair them with one major exception. In 1997 it was determined that replacing the COBOL based core accounting system, comprised of the general ledger and payroll systems, with a Y2K compliant enterprise accounting system could not be accomplished in the time remaining. The city engaged a consultant to modify the program code to accept year 2000 day calculations. These core accounting systems were tested and verified as Y2K ready in 1998.

The city has inventoried departmental computer systems, both hardware and software. Y2K readiness has been determined through a combination of vendor validation, system testing and third party consultant review. The city has employed verification and validation software to test all desktop user hardware and software for Y2K compliancy. Where appropriate, external computer interfaces have been validated. Examples include the city's 911 interface with the regional phone system and the city's financial interface with our primary bank.

One primary goal of the city's Y2K strategy is to ensure residents and businesses that the city of Santa Clara is working diligently on their behalf to minimize disruptions caused by the potential year 2000 computer problems. We've communicated our progress through a number of channels: Face-to-face meetings with major businesses and the Chamber of Commerce, regular updates posted on the city's website, cable cast over the city's Government channel, and printed in the city newspaper which is distributed to all residents and businesses. Additionally, we're in the process of holding a series of Y2K meetings throughout the community to update and advise neighborhoods on individual and family emergency preparedness. Over the next 3 months, we will be mailing out materials on home and small business preparedness for possible Y2K caused disruptions.

As we have moved in to the later portion of 1999, contingency planning has surpassed remediation as the primary Y2K focus for the city. We are both encouraged and assured by Y2K remediation efforts occurring in both the private and public sectors in the Silicon Valley, but we also understand our day-to-day reliance on complex, far-reaching interconnected computer systems. Given the millions of lines of programming code contained in these systems and the thousands of embedded chips that control these systems, we fully anticipate the possibility of Y2K disruptions in the community and the region as a whole. We are advising the community to prepare for possible Y2K disruptions much in the same manner as a household would prepare for an earthquake or flood threat. We are advising moderation in food and supply stockpiling and the amount of cash kept on hand. The Y2K preparedness checklist would contain certain unique characteristics such as advising households to keep hardcopy financial records for the later part of 1999. We do not believe Y2K preparedness needs to be dramatically different than typical household emergency preparedness.

The city has been preparing for possible Y2K disruptions through a series of tabletop exercises and problem simulations that allow staff to practice and perfect the emergency response systems. By the completion of this series of emergency exercises we will have involved agencies such as the school district, our local hospital and the Red Cross to enhance the ability to coordinate our emergency response. Additionally, the city departments are reviewing manual work-around procedures that would allow at least a basic level of city services to be maintained in critical areas if computer systems were to fail.

The city's emergency operation center will be open and fully staffed over the New Year's period. We will track Y2K related events over the Internet as they unfold through the dateline through Asia into Europe and across the Eastern United States. We will maintain a telephone bank to quickly respond to community concerns or rumors. In the event of a major regional disruption in electric power or communications, the city has fall-back alternatives available on a very localized basis. We are prepared for an extended Y2K response period if that becomes necessary.

In closing, I want to thank the committee for the opportunity to speak this morning. On behalf of the City Council of the city of Santa Clara, I extend our appreciation to the committee for your diligence and efforts in determining year 2000 readiness throughout this nation. Thank you.

Mr. HORN. Thank you. We appreciate your remarks.

[The prepared statement of Mr. Garratt follows:]

Year 2000 Readiness

Congress of the United States

House of Representatives
August 14, 1999

Committee on Government Reform
Subcommittee on Government Management, Information, and Technology

Efforts of State and Local Governments

And Businesses to

Address the Year 2000 Computer Problem

Testimony of

Ronald E. Garratt

Assistant City Manager

City of Santa Clara

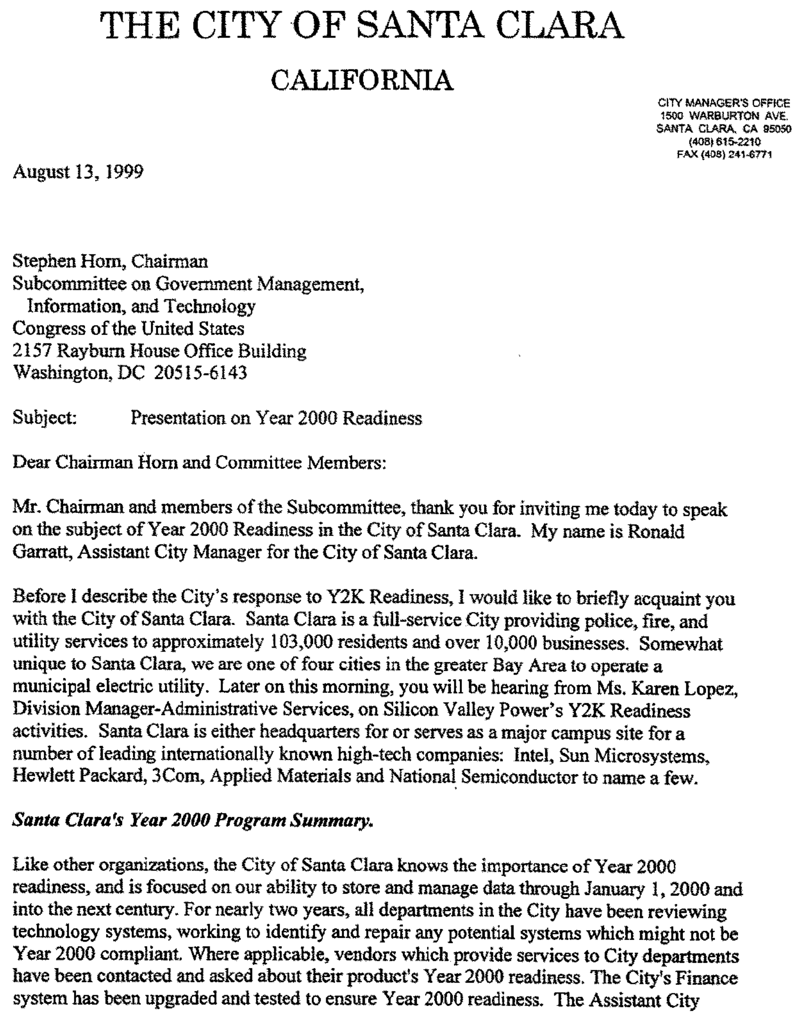
Biography of

RONALD E. GARRATT
ASSISTANT CITY MANAGER
CITY OF SANTA CLARA

Ron Garratt has been with the City of Santa Clara since 1988; the first two years with the Finance Department as Assistant Director of Finance and nine years in his current position as Assistant City Manager. He has also held budget and finance positions with the City of Palo Alto and Bureau of Labor Statistics, Washington, D.C. and taught business and accounting courses at the University of the South Pacific in Fiji while in the Peace Corps.

Ron oversees the coordination of major departmental projects for the City Manager's Department with particular emphasis on the leasing and management of City owned properties, economic development coordination, and management of the City's computer network.

Ron holds a Bachelor of Science degree is Business Administration from California State University, Hayward, and is a member of the International Right-of-Way Association.



THE CITY OF SANTA CLARA

CALIFORNIA

CITY MANAGER'S OFFICE
1500 WARBURTON AVE.
SANTA CLARA, CA 95050
(408) 615-2210
FAX (408) 241-6771

August 13, 1999

Stephen Horn, Chairman
Subcommittee on Government Management,
Information, and Technology
Congress of the United States
2157 Rayburn House Office Building
Washington, DC 20515-6143

Subject: Presentation on Year 2000 Readiness

Dear Chairman Horn and Committee Members:

Mr. Chairman and members of the Subcommittee, thank you for inviting me today to speak on the subject of Year 2000 Readiness in the City of Santa Clara. My name is Ronald Garratt, Assistant City Manager for the City of Santa Clara.

Before I describe the City's response to Y2K Readiness, I would like to briefly acquaint you with the City of Santa Clara. Santa Clara is a full-service City providing police, fire, and utility services to approximately 103,000 residents and over 10,000 businesses. Somewhat unique to Santa Clara, we are one of four cities in the greater Bay Area to operate a municipal electric utility. Later on this morning, you will be hearing from Ms. Karen Lopez, Division Manager-Administrative Services, on Silicon Valley Power's Y2K Readiness activities. Santa Clara is either headquarters for or serves as a major campus site for a number of leading internationally known high-tech companies: Intel, Sun Microsystems, Hewlett Packard, 3Com, Applied Materials and National Semiconductor to name a few.

Santa Clara's Year 2000 Program Summary.

Like other organizations, the City of Santa Clara knows the importance of Year 2000 readiness, and is focused on our ability to store and manage data through January 1, 2000 and into the next century. For nearly two years, all departments in the City have been reviewing technology systems, working to identify and repair any potential systems which might not be Year 2000 compliant. Where applicable, vendors which provide services to City departments have been contacted and asked about their product's Year 2000 readiness. The City's Finance system has been upgraded and tested to ensure Year 2000 readiness. The Assistant City

Manager and City consultants are tracking and monitoring progress in this area. The City is making its best effort to ensure that municipal data will be accurate and that services will continue satisfactorily beyond the Year 2000.

Highest priority has been placed on systems which control our Communications (9-1-1) systems and Police and Fire dispatch, and traffic control systems. In addition, our utilities have also been a major focus. The City's Electric Utility, Silicon Valley Power, has begun to replace or retrofit many of our critical systems. We have completed an inventory and assessment of all Silicon Valley Power equipment and data systems, and we will continue to address our electronic interfaces with other agencies. This assessment was completed in February 1999. With regard to our embedded systems, we have completed inventory and assessment. Our target for remediation of any problem embedded systems was met in June 1999.

Many other important computer programs are, or have been made, Year 2000 compliant, including the utility billing system and the water distribution and sanitary sewer conveyance control systems. The Water and Sewer Utilities continue to examine other Year 2000 mission critical exposures and the necessary corrections as deemed appropriate. Considering work performed to date, the Water & Sewer Utilities do not believe there will be any interruption of water or sanitary sewer service to our customers due to a Year 2000 problem under the control of the City. While it would not be as efficient to operate the water and sewer systems without certain computerized system control features, the City's contingency planning allows the systems to be manually operated, if necessary.

Technology Update.

The past few years have seen a significant growth in the use of technology in the City of Santa Clara:

- In 1994 there were approximately fifty employees connected to a narrowly defined local area network (LAN) for the primary purpose of file sharing. Today there are over 700 City employees connected to a centralized Wide Area Network (WAN) providing e-mail services, document sharing, consolidated calendaring and a common application product that provides text processor, spreadsheet, database, and presentation software for every connected employee.
- A few years ago only a handful of employees had access to the Internet. Today hundreds of employees have Internet access and communicate regularly with customers and citizens.
- The City has established a Web site which is continually expanded and enhanced to keep up with the growing demand for information from the community. The Web site has grown to over 3,000 pages with 250 screens containing a pre-addressed "send a message" button to communicate with City Hall. The City's Web site is receiving between 3,000

and 5,000 user sessions per month, resulting in approximately 80,000 "hits" to the various screens. The Human Resources Department screens receive the most hits each month, approximately 2,600 due to user's seeking employment opportunities.

- Operating departments have made a major effort to replace obsolete automated systems with new applications containing far more functionality and ease of use and maintenance. Approximately $22 million has been spent on technology project upgrades and replacements over the past five years (see Exhibit A). System upgrades and enhancements are planned well beyond the year 2000 (see Exhibit B).

Year 2000 (Y2K) Problem.

The Y2K problem has been so extensively discussed in the news this past year that the term "Y2K" has come into common usage in the public's vocabulary. Y2K is also referred to as the Millennium Bug or the Year 2000 problem. The issue relates to how computers read dates. Early programming language abbreviated dates as the last two digits in a year to save expensive memory storage. The year 1965 would be read by the computer as "65". Computer code understood the first two digits to be "19". It was felt thirty to forty years ago that this code would be replaced by more sophisticated programming by the turn of the century.

Unfortunately, many of the early computer systems are still in use. There is a concern that when these systems attempt to read the date on January 1, 2000 they will interpret "00" as 1900, not 2000. This would produce chaos in programs set to calculate financial transactions, maintenance routines, date sensitive programs, etc. Additionally, there are "embedded chips" in many common products in use today (personal computers, VCR's, microwaves, telephones, automobiles, etc.). Some of these chips are date sensitive and may fail to work on or after January 1, 2000. For many cases people are not aware that a particular item has an embedded chip in it. Industry experts predict that of the 25 billion chips in electronic components, only about 2 percent will fail due to the devices losing track of their timing function. But there is no way to know which 2 percent.

The City's Y2K Strategy.

The City is working aggressively towards being a Y2K ready organization for all major systems no later than September 1999 with the exception of two departmental operating systems which will be implemented November 1999. The goal is to ensure that all functions will be operating and interacting normally into the year 2000 and beyond. The City is working to ensure that our automated systems will process normally, as designed, before, during and after January 1, 2000. The City views the Y2K issue as both a technical problem and a business risk. This risk focuses on:

- Individual programs, applications, and systems.
- Application integration across two or more systems and applications.

- Enterprise network and hardware infrastructure.
- Supplies, financial institutions, other government agencies and upstream utility providers.
- Non-information technology systems such as telephone service, security systems, etc.

Fix or Replace Options.

The two primary options considered to reach Y2K readiness are renovation, where an application, system or computerized component is fixed or modified to become Y2K ready and replacement, where non-Y2K ready resources are replaced with compliant, purchased solutions.

The City has chosen replacement as the method of choice for Y2K readiness. Twenty-Two million dollars ($22 million) has been allocated over the past five years for systems replacement. Many of these fix or replace decisions were made in the early 1990's, not driven by Y2K compliance, but rather because many of these COBOL based programs lacked features and capabilities available and desired by operating departments.

Some COBOL programming fixes have been performed, most significantly to the City's financial management information system. These code modifications were made by the system's original vendor with extensive parallel testing and mock runs and certified Y2K ready in 1998.

City's Y2K Project Team.

Due to the importance of the Y2K issue the City Manager assigned overall coordination of Y2K readiness to her office, under the direction of the Assistant City Manager. All departments participate in the project with the City's contracted computer facilities manager and a third party consultant advising on and reviewing the work effort. Due to heightened concern over availability of electric power throughout the western states power grid, Silicon Valley Power has created a departmental Y2K readiness team led by their Division Manager for Administrative Services. As with other City departments, Silicon Valley Power has engaged a Y2K consulting firm to assist in the process. The use of external consultants broadens the City's knowledge and ability to employ best practices in meeting our Y2K objectives.

Y2K Project Activities.

The City's Y2K readiness team works in close coordination with Silicon Valley Power's Y2K readiness team. Activities to date include:

- Establishment of the Project Teams
- Development of Guidelines and Policies
- Education and Awareness
- Inventory and Assessment
- Remediation or replacement
- Testing

Activities that are ongoing or to be completed at a future date include:

- Continued Verification and Validation Testing
- Contingency Planning

Education and Awareness.

Silicon Valley Power has done an excellent job in communicating the utility's Y2K progress to date by holding a series of meetings with its' major customers. The City will continue to post and update Y2K information on the City's Web Site (www.ci.santa-clara.ca.us) and in the City's community newspaper, "Inside Santa Clara". The City has utilized Mission City Scenes and Cable Channel 6/15 to communicate relevant Y2K information to the community. Additionally, staff continues to return to the City Council for periodic updates on our Y2K remediation efforts. Community outreach efforts both completed and planned, are extensive (see Exhibit C).

Y2K Legal Liabilities.

The potential effects of the Year 2000 problem are creating an environment in which legal action may be unavoidable. Many companies are sending Y2K compliance letters to suppliers for a risk assessment response. Unfortunately, the inconsistency of approach taken in constructing these letters often requires the receiving company to establish a common response, usually not in conformance with the check-off box methodology requested by the sending company.

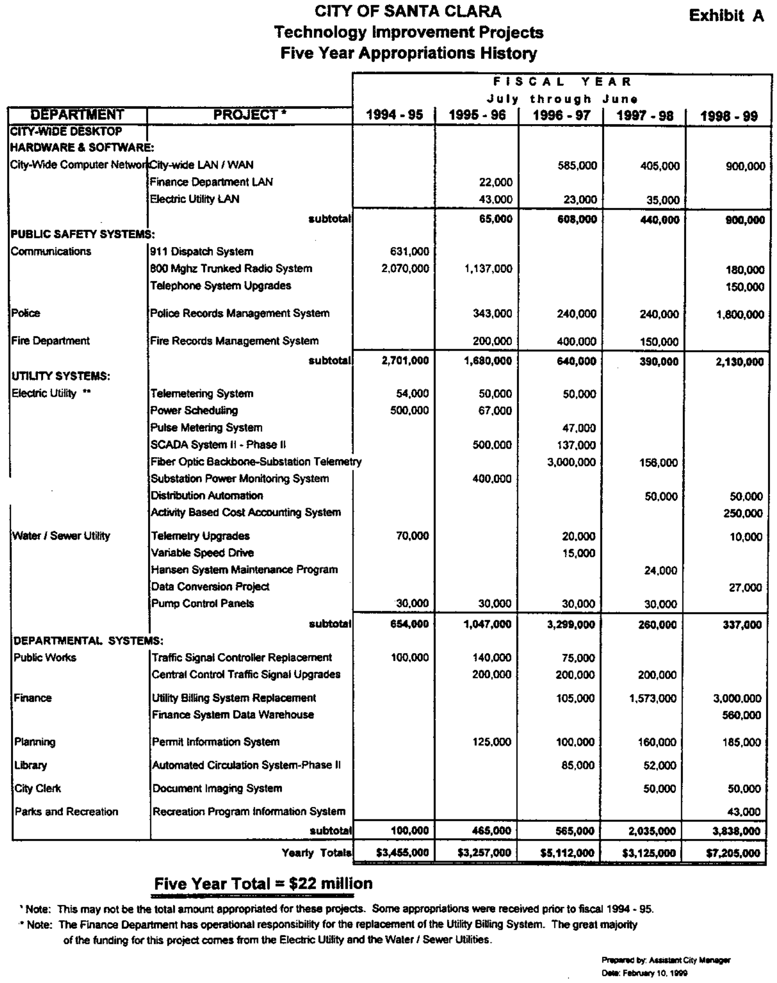
Of the approximately two hundred letters received by the City to date, nearly all are interested in the viability of the electric system with approximately 20% querying the Y2K readiness of the water/sewer utility. It is the City's position to be responsive to our customers while at the same time demonstrating our due diligence in resolving our Y2K issues.

Contingency Planning.

As we move further into 1999, contingency planning has surpassed remediation as the primary Y2K effort for the City. Staff has commenced the process of developing plans to minimize service disruptions and restore necessary services, if required. Contingency planning is City-wide and takes off from the City's standing practice of regularly testing our emergency operations capabilities. Activities to date include:

- Two City-wide table top exercises that focused on selected Y2K problem scenarios.
- Notification to senior management that the City's Emergency Operations Center (EOC) will be activated for the period before, during, and after January 1, 2000.
- Ongoing research into the use of selected Internet sites to track Y2K events as they evolve from the international dateline to the west coast of the U.S.
- Ongoing development and practice of semi-automated or manual "work arounds" in the event of the failure of critical systems that impact service delivery to the community.
- Meeting meet with key community service providers, such as the Santa Clara Unified School District, to discuss readiness plans.

In closing, I want to thank the Committee for this opportunity to speak. On behalf of the City Council of the City of Santa Clara, I extend our appreciation to the Committee for your diligence and efforts in determining Year 2000 Readiness throughout this nation.



CITY OF SANTA CLARA
Technology Improvement Projects
Five Year Appropriations History

Exhibit A

		FISCAL YEAR July through June				
DEPARTMENT	PROJECT *	1994 - 95	1995 - 96	1996 - 97	1997 - 98	1998 - 99
CITY-WIDE DESKTOP HARDWARE & SOFTWARE:						
City-Wide Computer Networ	City-wide LAN / WAN			585,000	405,000	900,000
	Finance Department LAN		22,000			
	Electric Utility LAN		43,000	23,000	35,000	
	subtotal		65,000	608,000	440,000	900,000
PUBLIC SAFETY SYSTEMS:						
Communications	911 Dispatch System	631,000				
	800 Mghz Trunked Radio System	2,070,000	1,137,000			180,000
	Telephone System Upgrades					150,000
Police	Police Records Management System		343,000	240,000	240,000	1,800,000
Fire Department	Fire Records Management System		200,000	400,000	150,000	
	subtotal	2,701,000	1,680,000	640,000	390,000	2,130,000
UTILITY SYSTEMS:						
Electric Utility **	Telemetering System	54,000	50,000	50,000		
	Power Scheduling	500,000	67,000			
	Pulse Metering System			47,000		
	SCADA System II - Phase II		500,000	137,000		
	Fiber Optic Backbone-Substation Telemetry			3,000,000	156,000	
	Substation Power Monitoring System		400,000			
	Distribution Automation				50,000	50,000
	Activity Based Cost Accounting System					250,000
Water / Sewer Utility	Telemetry Upgrades	70,000		20,000		10,000
	Variable Speed Drive			15,000		
	Hansen System Maintenance Program				24,000	
	Data Conversion Project					27,000
	Pump Control Panels	30,000	30,000	30,000	30,000	
	subtotal	654,000	1,047,000	3,299,000	260,000	337,000
DEPARTMENTAL SYSTEMS:						
Public Works	Traffic Signal Controller Replacement	100,000	140,000	75,000		
	Central Control Traffic Signal Upgrades		200,000	200,000	200,000	
Finance	Utility Billing System Replacement			105,000	1,573,000	3,000,000
	Finance System Data Warehouse					560,000
Planning	Permit Information System		125,000	100,000	160,000	185,000
Library	Automated Circulation System-Phase II			85,000	52,000	
City Clerk	Document Imaging System				50,000	50,000
Parks and Recreation	Recreation Program Information System					43,000
	subtotal	100,000	465,000	565,000	2,035,000	3,838,000
	Yearly Totals	$3,455,000	$3,257,000	$5,112,000	$3,125,000	$7,205,000

Five Year Total = $22 million

* Note: This may not be the total amount appropriated for these projects. Some appropriations were received prior to fiscal 1994 - 95.

** Note: The Finance Department has operational responsibility for the replacement of the Utility Billing System. The great majority of the funding for this project comes from the Electric Utility and the Water / Sewer Utilities.

Prepared by: Assistant City Manager
Date: February 10, 1999

CITY OF SANTA CLARA

Exhibit B

Technology Improvement Projects - Five Year Financial Plan

		FISCAL YEAR July through June				
DEPARTMENT	PROJECT	1999-00	2000-01	2001-02	2002-03	2003-04
CITY-WIDE DESKTOP HARDWARE & SOFTWARE:						
City-wide Computer Network	City-wide Data Communications Network	$ 1,000,000	$ 1,000,000	$ -	$ -	$ -
	City-wide Data Comm. Network 01-05	-	-	1,000,000	1,000,000	1,000,000
	subtotal	1,000,000	1,000,000	1,000,000	1,000,000	1,000,000
PUBLIC SAFETY SYSTEMS:						
Communications	Dispatch & Central Electronics Bank Upgrade	96,000	-	-	-	-
	EMD/PAI Dispatch Program Implementation	125,000	-	-	-	-
	Telephone System Upgrades	175,000	175,000	-	-	-
	CAD System Major Revision Upgrade	425,000	-	-	-	-
	Institutional Telecommutions Network (I-Net)	711,000	237,000	237,000	237,000	237,000
Fire Department	Fire Records Management System	150,000	-	-	-	-
	Traffic Pre-emptors 95/96 - 99/00	52,000	-	-	-	-
	Traffic Pre-emptors 00/01 - 04/05	-	64,000	70,000	76,000	84,000
	subtotal	1,734,000	476,000	307,000	313,000	321,000
UTILITY SYSTEMS:						
Electric Utility	Direct Access	150,000	-	-	-	-
	Year 2000 Readiness	150,000	-	-	-	-
	subtotal	300,000	-	-	-	-
DEPARTMENTAL SYSTEMS:						
Public Works	Traffic Signal Controller Replacement	-	75,000	75,000	75,000	75,000
	Central Control Traffic Signals Phase XIII A	-	200,000	-	-	-
	Computerized Irrigation Control System	215,000	215,000	215,000	215,000	-
Finance	Utility Management Information System	3,500,000	1,500,000	-	-	-
	Financial System Data Warehouse	600,000	200,000	8,000,000	-	-
	Finance Document Imaging System	100,000	-	-	-	-
Planning	Geographic Information System	133,400	-	-	-	-
	Permit Information System Phase II	149,400	50,000	100,000	25,000	25,000
	Geographic Information System Phase II	-	50,000	50,000	75,000	50,000
Library	Automated Circulation System - Phase III	114,700	73,900	13,400	45,400	40,000
	Library Security & Selfcheck System	73,370	58,420	30,785	40,570	30,785
City Clerk	Public Document Access System	30,000	-	20,000	20,000	20,000
Parks and Recreation	Recreation Program Information System	-	-	30,000	-	-
	subtotal	4,915,870	2,422,320	8,534,185	495,970	240,785
	Yearly Totals	$ 7,949,870	$ 3,898,320	$ 9,841,185	$ 1,808,970	$ 1,561,785

Five Year Projection = $25,060,130

Prepared by: Finance
Date: March 5, 1999

CITY OF SANTA CLARA

Year 2000 Readiness – Community Outreach

1. Cover (back cover) article in Inside Santa Clara municipal newspaper, Spring (March 1), 1999, mailed to all residential addresses in the City.

2. Cover (front cover) article in Inside Santa Clara municipal newspaper, Summer (June 1), 1999, mailed to all residential addresses in the City.

3. Letters to businesses from City Manager's Office

4. Article in June, 1999 City Corner employee newsletter distributed to al employees (to educate them on City efforts so that they can provide public information, and to educate them on how to be prepared, themselves)

5. Presentations to the City Council (televised for cable customer access) reviewing the City's Y2K preparedness.

6. Information on the City's website (reprints from reports to Council, etc.)

7. June 23 community meeting at Central Library (to be videotaped)

Planned (as we approach 1-1-00):

8. Subsequent community meeting at location North of Bayshore Freeway (also to be videotaped).

9. Videotape using clips from community meetings to be broadcast on Mission City TV (the City's government access channel 15) at scheduled times during through the remainder of 1999

10. Periodic announcements on Mission City TV (the City's government access channel bulletin board).

11. Article in the Fall, 1999 Recreation Activities Guide, distributed to all residential addresses in August, 1999

12. Articles in Fall (September 1) and

13. Winter (December 1) Inside Santa Clara newspaper, with expanded delivery beyond all residential addresses to include all businesses, too

14. Article in September, 1999 Mission City SCENES municipal utility bill insert distributed to all residents and businesses.

15. Article in October, 1999 City Corner employee newsletter with updated info to all employees.

16. Brochure to be distributed at community events and placed at public counters.

17. Post card mailings to all addresses in the City

18. Advertisement in local weekly newspaper.

Exhibit C

Mr. HORN. Christiane Hayashi is the year 2000 communications manager for the city of San Francisco. Thank you for coming.

Ms. HAYASHI. Thank you, Mr. Chairman, I want to thank the subcommittee for the opportunity to participate in the national dialog on this topic. I also want to take the opportunity to personally thank the General Accounting Office for all the invaluable information that they have passed along that has been of use to the State and local governments, and I'm sure even private businesses as well.

I brought with me as written testimony a rather long report to the San Francisco Board of Supervisors. Unfortunately it was prepared as an internal document and it's hot off the presses. I didn't get a chance to repackage it for external viewing. So the only clue that it's from San Francisco is the CCSF acronym at the top corner of the page. I apologize for that. We'll take care of that when we get back to the office.

Mr. HORN. When you say it's an internal document, you can be sure the press will want that one more than any.

Ms. HAYASHI. There are 75 copies on the table, so everyone's welcome to it. It's a document that we prepared. It's the most recent Y2K status for the San Francisco Board of Supervisors, and it contains detailed status reports for each of the 14 mission-critical departments in the city as designated for the focus of this Y2K preparation. But actually, I'd like to talk about something that's not in that report, and I'd be happy to take any specific questions on status as well.

Everyone who's dealt with Y2K for any period of time can rattle off the improved procedures, inventory assessment, remediation, testing, contingency planning, supplier verification, and most recently identified some elements of due diligence as independent validation and verification, and the city is, of course, actively engaged in this process. But what has emerged as one of the most important elements of Y2K preparation is public awareness.

It's become apparent to many jurisdictions as you've heard in prior testimony that whether Y2K has seriously harmful effects to society could depend on the individual citizen's level of preparation for it and how they react to it. And by public awareness, I mean, first of all, that we get accurate information to the public so that they can evaluate whether their government's efforts are addressing all of their needs in a due diligence process, and so that the public can share the Government's confidence when certain systems are certified as Y2K ready, and also so that each person and household can assess what their risks are based on their personal needs and priorities. For example, the person who requires medication might assess the risks to the pharmaceutical industry and decide how much medication to keep around the house in the event of need.

And also by public awareness, I mean that we get information to the public about how they should prepare. At this point, enough agencies and businesses have accomplished enough work so that those following Y2K progress are breathing a little easier about the potential effects of New Year's Eve on the social and economic fabric of the United States, at least from a technical perspective, although we do recognize much work remains to be done.

The banking and utility industries and their associated regulatory agencies have expressed pretty good levels of confidence that their services will continue uninterrupted. Consumer automobiles have been warranted by the manufacturers and most central systems of public and private organizations will have received at least some attention by the end of the year. Most governments have achieved substantial readiness and rapid progress continues.

But the fact remains that we can expect some surprises from Y2K, and a significant danger remains that a public panic reaction could have severely detrimental effects. People need to understand that they can expect Y2K-related headaches in the first half of next year, so that they shouldn't run screaming into the streets the first time that the lights flicker. They also need to take advantage of this opportunity to prepare to be just a little bit self-reliant.

Personal Y2K preparation is like buying fire insurance. Is it likely that your house will burn down? Not really, but there is a chance, and the value of your home and its contents are sufficiently important that you take the time and spend the money to protect it against that eventuality. Having purchased that fire insurance, you can feel secure that come the worst, you have some protection.

Similarly in the Y2K context, it's looking very unlikely that there will be serious infrastructure breakdowns. However, because of the complex interdependencies of our high-tech society, what could fail and for how long remains a great uncertainty. Just as agencies have looked over their inventories assessing the compliance, fixed their non-compliant systems, tested their fixes and made back-up plans, so the citizens should identify their personal priorities for the mission-critical systems, like insulin to a diabetic. They should assess their risk of failure of those systems such as checking the websites of the manufacturers of the elements that you might have at home. They should fix what they can, such as downloading fixes for their personal computing systems from manufacturer's websites, and they should identify the alternatives to those things that could fail, but are beyond their individual capacity to fix, such as keeping a supply of essential and nonperishable groceries of the household needs.

Above all, people should be prepared for Y2K by remaining rational and avoiding hysteria about the millennium. Panic could result in long-term economic problems, rioting, looting and other socially unproductive behavior. Now is the time for people to remember that we are low-tech human beings. There's nothing standing between us and the earth and the sunlight and the air we breathe. Our families and friends don't have computer chips. Our social network will remain intact. Since no one has ever suggested that Y2K will result in spontaneous combustion, we should have most of our personal possessions around us.

With just a little bit of preparation, we can provide ourselves with Y2K insurance. In California where we've had at least three major earthquakes, raging fires, power outages and alternating drought and floods during this century, it's merely common sense to make your household self-reliant in a few fundamental respects: Nonperishable food, water, necessary medicine, flashlights, a little cash, security of important documents.

But for ourselves and each other, we can use this fascinating Y2K historical event as an opportunity to strengthen our human bonds and improve our collective future. That's the message of optimism and personal empowerment that we feel is an important part of San Francisco's readiness effort. Thank you.

Mr. HORN. Well, thank you. That's very well stated, and you are right on the mark, and as I listen to you, I think you probably get the last word when you see the mayor who is used to having the last word. So thanks for coming and sharing those insights with us. We appreciate it.

[The prepared statement of Ms. Hayashi follows:]

CCSF Y2K Program Management Office

YEAR 2000 READINESS STATUS REPORT

Board of Supervisors' Report
August 12, 1999

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In 1995 the City had its first organized Year 2000 (Y2K) training session. We had started to experience Y2K issues at places like Adult Probation where probation periods were extending past 1999. Information Technology professionals started working on the issue. In 1996, the first meeting of City department heads was called to discuss the issues and educate department heads on the risks of Y2K non-compliance.

Since that time, all major programs that run on City computers have been reviewed, tested and, where necessary, upgraded or replaced. A few of these programs are in the final remediation and retesting phase.

After several years of working on application systems, the risk of failure due to "embedded systems" became the focus of our activities. Embedded systems can be computer chips that are date-sensitive in street lights, elevators, biomedical devices and other equipment we rely on. Much of our efforts over the past year have been focused on doing inventories of these systems, assessing the risk of failure, upgrading or replacing and finally testing to make sure these systems will not fail.

In addition to doing all we can to avoid risk, City departments have been actively preparing or updating contingency plans. Even with the best preparation things can go wrong. In our daily business we rely on others for power, phone, banking and various other services. Departments have been working on plans that will still protect our citizens if these other possibilities become reality.

And finally, to guarantee that we will be prepared from citywide perspective, we have established a City Y2K project. We have hired an outside firm to audit, assess and assist our departments in their readiness efforts.

The Y2K Program Management Office (PMO) was created to serve as a centralized planning and assistance group to provide guidance and resources to City departments. The primary departments targeted by the PMO are those departments that provide mission-critical services to the City and County of San Francisco residents. The ultimate responsibility for departmental operations and Y2K readiness remains with the department heads. Additionally, the PMO has the responsibility for reporting on the City's overall Y2K readiness status to the Y2K subcommittee of the Committee on Information Technology (Subcommittee), the Board of Supervisors, the Mayor and the public. It serves as the single point of contact on the City's Year 2000 efforts.

Each of the fourteen mission-critical departments takes seriously the potential for Y2K related problems. These departments are inventorying, assessing, testing, remediating and preparing contingency plans. The City is committed to attaining a high level of confidence in the continuity of mission-critical services into the millenium. "Mission-critical" is defined as those services or functions, which, if disrupted, would have a direct and immediate impact on a citizen's health, safety or transportation. Examples of mission-critical services include public transportation, police, fire and medical emergency response, and utility services provided by the City. The PMO has divided mission-critical services into five categories:

CATEGORY	**DEPARTMENT**
PUBLIC SAFETY	Police Department Sheriff's Department Fire Department Mayor's Office of Emergency Services
PUBLIC HEALTH	Department of Public Health Department of Human Services
TRANSPORTATION	SF Municipal Railway SF International Airport Department of Parking and Traffic
UTILITIES	Public Utilities Commission
OTHER	Department of Telecommunications and Information Services Department of Purchasing Department of Real Estate Department of Public Works

PHASE I

In its first six months of operation, the PMO focused on the establishment of Y2K Project Managers and committees in each mission-critical department, providing guidelines and methodologies for the department's use. The PMO furnished training and assistance, as requested by departments, to meet their year 2000 readiness plans, track and monitor progress of the departments and report progress to the Subcommittee. An internal and external Y2K web page (www.ci.sf.ca.us & www.ci.sf.ca.us/y2k/internal) was developed to inform and educate the community about the City's efforts and to assist City departments in achieving Y2K preparedness.

Attached are the *Mission-critical Department's Y2K Status Reports* that discuss their progress. Each has reported that they are reviewing potential Y2K issues arising from embedded chips, information technologies, and vendor/supplier preparedness. Additionally, departments are working on contingency planning with the assistance of the PMO and focusing on component and system work-arounds in the case of dysfunction. The Mayor's Office of Emergency Services (MOES) is responsible for contingency planning for disaster-related issues associated with the new millennium. MOES and the SFPD have been developing an (*Incident Action Plan*) for the New Year's Eve weekend to ensure that City services are able to react quickly to any potential problems. As part of this process, MOES has hosted numerous planning meetings, and has conducted a number of exercises related to potential Y2K problems.

Some examples of the City's mission-critical department Y2K readiness as reported by the departments:

- Vehicles used by the Police Department have been assessed by the City and County's Purchasing Department which has indicated that standard equipment in SFPD Patrol cars will be unaffected by Y2K problems. Motorcycles do not use date-sensitive chips and are therefore Y2K ready.
- Jail doors, which rely on power, have been assessed by the Sheriff's Department to be Y2K ready. Jail locks have manual (key) overrides. Each facility is equipped with emergency back-up generators for power.
- Existing 911 and dispatch related systems are reported by the department as Y2K ready.
- The Fire Department's trucks and engines have been assessed by the department to be either unaffected by Y2K issues or are Y2K ready.
- Generators are deemed Y2K compliant by their vendors as they are electromechanical systems which are not date dependent.

- The Welfare Case Data System (Medi-Cal, Food Stamps Eligibility, Cash Assistance, and Welfare-to-Work) has been certified as Y2K compliant by the vendor, EDS. Therefore, services to clients will be uninterrupted.

- The Case Management Information and Payroll System (supports In-Home Supportive Services) has been successfully upgraded by the State in late July and will be in full production statewide effective August 2nd. Services to elderly and disabled individuals,as well as payment to care providers, will be uninterrupted.

- The Child Welfare System has been certified as Y2K compliant by the vendor, IBM, and the State's Health and Welfare Data Center. State mandated, time sensitive services that ensure safety of children in our custody should not be effected.

- Municipal Railway's Electric Trolley Coach, Bus Maintenance Garage at Flynn, Radio System, and Diesel Busses have all been found to be Y2K ready.

- The Federal Aviation Administration certified the Airport to be Y2K ready. All 13 of the critical life, safety and security systems, including fire alarms, security checkpoint system, carbon monoxide monitoring, call boxes, portable X-ray system and rescue and fire fighting trucks, are Y2K ready.

- All ground transportation and airfield operations systems are Y2K ready at the Airport.

- Parking and Traffic's signal controllers and master system clocks are deemed Y2K ready by the department.

- All major patient care systems for Department of Public Health, including the Shared Medical Systems (SMS) suite of products used by the Community Health Network, are Y2K ready. There is no anticipation of disruption in services for San Francisco General Hospital and Emergency Room, district health centers and all area patient specialty clinics.

- In mid-November, the existing Fire Department's 911 system will be replaced by a new system. The contract for the new 911 system requires all software and hardware to be Y2K compliant and the City criteria for accepting the new system includes system-wide testing for Y2K compliance.

To find additional examples of the City's Y2K readiness as reported by the departments, please look in the Mission-critical Departments' Y2K Readiness Status section.

PHASE II

The PMO entered Phase II of the citywide Y2K project on July 1, 1999, the beginning of the new fiscal year. This phase initiates independent verification and validation audits of the departments' embedded systems by a team of third party professional engineers. The industry standard among government agencies is to have independent verification and validation completed on mission-critical services. Phase II of the project will provide an additional level of departmental assistance, substantiation and confidence.

What follows is the PMO's independent verification and validation status reports of the fourteen mission-critical departments.

Airport

The PMO has completed the independent verification and validation high level review of Airport embedded systems. The Airport has put forth a significant effort to evaluate all of its mission-critical services as defined by the PMO, Federal Aviation Administration and the Air Traffic Controllers. The Airport has demonstrated a diligent and effective effort at inventory, assessment, testing, and certifying compliance of the mission-critical services that support airfield operations, terminal operations, ground transportation, and life, safety and security systems. The PMO has confidence in the Year 2000 readiness of the Airport.

Department of Telecommunications and Information Systems (DTIS)

The PMO is assisting DTIS with a variety of their projects that support mission-critical services. Because of the criticality of the services they provide, we are conducting a full independent verification and validation of the crucial systems. The PMO will continue working closely with the department.

Emergency Communications Department

The new 911 system is scheduled to come online with the Fire Department in mid-November. Although the new system is under contract to be verified as Y2K compliant on a component level and tested system-wide as Y2K compliant, the PMO will conduct independent verification and validation of mission critical systems.

Emergency Services

The Mayor's Office of Emergency Services maintains extensive contingency plans for use in emergencies and Emergency Operation Center systems are designed to be redundant. Despite this and due to the criticality of the service, the PMO plans to conduct an independent verification and validation in August.

Fire Department

The PMO recently began the process of conducting a complete independent verification and validation of their embedded system inventory to ensure the highest level of readiness for the City and County of San Francisco.

Human Services

The PMO is in the process of independently verifying and validating DHS's Y2K readiness. The PMO has currently reviewed 50% of their systems, and from the preliminary finding reports that DHS has done extensive Y2K preparation.

Municipal Railway

Due to the department's criticality, we are engaged in a full independent verification and validation of all their mission-critical systems. The PMO is currently 40% done with this effort, and to date, the results are reassuring for systems that the PMO has reviewed.

Parking and Traffic

The PMO has scheduled an independent verification and validation of the department's mission-critical services in August.

Police

The PMO recently started an independent verification and validation of the department. To date, the audit has focused on other departments that provide crucial systems affecting the Police Department's ability to provide mission-critical services. The PMO is validating that "owning" departments, such as DPW, Purchasing, and DTIS (for example), are Y2K ready.

Public Health

The PMO has found that DPH has diligently and effectively reviewed their mission-critical systems for Y2K readiness. To date, the PMO is 75% completed with the independent verification and validation of their mission-critical services.

Public Utilities Commission

The PMO recently began the initiative to independently review the PUC' s mission-critical systems and their Y2K readiness. We are in the process of conducting a complete independent verification and validation of their embedded system inventory to ensure the highest level of readiness for the City and County of San Francisco.

Public Works

DPW is responsible for numerous buildings that have been deemed mission-critical. The PMO's independent verification and validation of their Y2K readiness is 10% complete.

Purchasing

The PMO has scheduled an independent verification and validation of the department's mission-critical services in August.

Real Estate

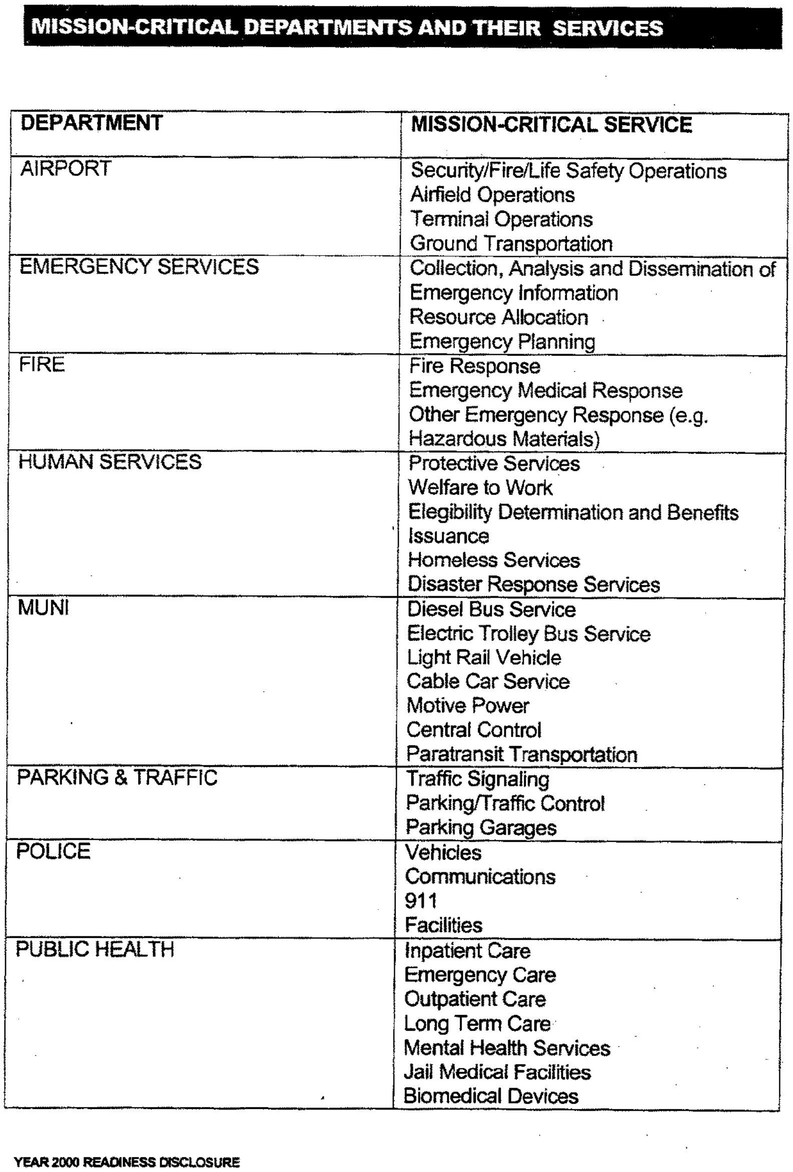
Independent verification and validation has not been scheduled at this time.

Sheriff

The PMO recently began the process of conducting a complete independent verification and validation of their embedded system inventory to ensure the highest level of readiness for the City and County of San Francisco.

The City and County of San Francisco continues to demonstrate their commitment to providing uninterrupted service on January 1, 1999 by conducting independent verification and validation of mission-critical services. The PMO will carry on assisting and monitoring their Y2K readiness.

What follows are the Y2K status reports as given by the fourteen mission-critical departments.



MISSION-CRITICAL DEPARTMENTS AND THEIR SERVICES

DEPARTMENT	MISSION-CRITICAL SERVICE
AIRPORT	Security/Fire/Life Safety Operations Airfield Operations Terminal Operations Ground Transportation
EMERGENCY SERVICES	Collection, Analysis and Dissemination of Emergency Information Resource Allocation Emergency Planning
FIRE	Fire Response Emergency Medical Response Other Emergency Response (e.g. Hazardous Materials)
HUMAN SERVICES	Protective Services Welfare to Work Elegibility Determination and Benefits Issuance Homeless Services Disaster Response Services
MUNI	Diesel Bus Service Electric Trolley Bus Service Light Rail Vehicle Cable Car Service Motive Power Central Control Paratransit Transportation
PARKING & TRAFFIC	Traffic Signaling Parking/Traffic Control Parking Garages
POLICE	Vehicles Communications 911 Facilities
PUBLIC HEALTH	Inpatient Care Emergency Care Outpatient Care Long Term Care Mental Health Services Jail Medical Facilities Biomedical Devices

	Hazardous Materials Community-wide Emergency Response
PUBLIC UTILITIES COMMISSION	Water Distribution Water Treatment Wastewater Collection Wastewater Treatment Power Generation Power Distribution
PUBLIC WORKS	Operation of Buildings and Facilities maintained by the Bureau of Building Repair Emergency and Disaster Response Street Maintenance and Repair
PURCHASING	Vehicle Maintenance and Repair Vehicle Fueling Machine Shop Services Purchase/Procurement of Goods/Services OES Logistics Support
REAL ESTATE	Leased Facility Management
SHERIFF	County Jails: Intake/Release/Housing Inmate Transportation Security Services: City Hall / Courts / CAD911
TELECOMMUNICATIONS AND INFORMATION SERVICES	Enterprise Computing Services Computer Applications Telecommunication Services

[redacted]

MISSION-CRITICAL DEPARTMENTS' Y2K STATUS REPORTS

San Francisco International Airport

The San Francisco International Airport has identified the following services as mission-critical:

Security/Fire/Life Safety Operations

Airfield Operations

Terminal Operations

Ground Transportation

The San Francisco International Airport (SFO) has implemented an Airport-wide program to review and prepare its computer systems, embedded systems and components for the year 2000. The Y2K readiness program of the Airport focuses on critical areas of operation including airfield, terminal, transportation, security, communications and financial systems. Inventory, assessment and compliance activities to identify and remediate all mission-critical and essential systems have been completed. Fuel service for Airport motor vehicles is expected to be Y2K ready by September 30, 1999.

SFO reports that thirteen systems make up the Life Safety and Security Systems. These systems include airport fire alarms, security checkpoint system, carbon monoxide monitoring and call boxes, portable X-ray system, and rescue and fire fighting trucks. SFO reports that all 13 of these systems are Y2K ready.

There are two systems under the Ground Transportation category. These two systems, traffic light control and parking control, are currently reported as being Y2K ready.

SFO currently reports that there are three systems that support Airfield Operations. These systems are airfield lighting, fuel delivery (airlines) and Multi-User System Environment (MUSE) Gate Scheduling System. SFO reports these systems are Y2K ready. These systems have been successfully tested or have sufficient vendor documentation of Y2K readiness, which has been signed off by SFO.

Terminal Operations are supported by fourteen systems including HVAC, fuel services (airport), baggage system and backup power systems. Of the fourteen, 13 are currently Y2K ready. The remaining system, which supports fuel delivery for airport motor vehicles, is currently being evaluated for Y2K readiness by the vendor.

Mayor's Office of Emergency Services (MOES)

The Mayor's Office of Emergency Services has identified the following as mission-critical:

Collection, Analysis and Dissemination of Emergency Information
Resource Allocation
Emergency Planning

The Mayor's Office of Emergency Services has responsibility for the City's Emergency Operations Center and is heavily dependent on support from City agencies and other outside agencies such as the State of California.

MOES is currently migrating its computer operations from a non-compliant server to an administrative server administered by the Emergency Communications Department. As part of this process, MOES replaced staff computers and has preformed the necessary upgrades to ensure compliance. MOES is also installing a new Y2K compliant file server and Thin Client software to support the Emergency Operations Center (EOC) and is performing upgrades on the EOC computers.

MOES has been in touch with the Governor's Office of Emergency Services to insure compliance of the State's Operational Area Satellite Information System (OASIS) and Emergency Digital Information System (EDIS). While MOES has not received a statement from the State yet, both systems are expected to be compliant by November. MOES has also purchased satellite telephone systems to parallel the State's OASIS system. The Emergency Alert System that is used in parallel with EDIS is Y2K ready.

As an emergency services agency, MOES maintains extensive contingency plans for use in emergencies and EOC systems are designed to be redundant. Plans include provisions for completely relocating the EOC to a new location and for the use of manual systems for emergency operations. In addition, MOES and the SFPD have been developing an Incident Action Plan for the New Year's Eve weekend to ensure that City services are able to react quickly to any potential problems. As part of this process, MOES has hosted numerous planning meetings and has conducted a number of exercises related to potential Y2K problems.

Fire Department

The San Francisco Fire Department (SFFD) has identified the following as mission-critical:

Fire Response
Emergency Medical Response
Other Emergency Response (e.g. Hazardous Materials)

The SFFD is making substantial progress in addressing its Y2K issues. Inventory of both information technology (IT) and facilities related systems are now complete. Inventoried IT systems include computer aided dispatch, Automatic Vehicle Location System (AVLS), and auxiliary water supply, among others. All Fire Department facilities were inventoried. The facilities inventory consists of over 400 entries representing 55 unique devices. The completeness of the inventory and readiness of these devices is currently being verified by PMO engineers.

All mission-critical IT systems have been assessed and remediation and testing are currently underway. Existing 911 and dispatch related systems are reported by the department as Y2K ready.

Facilities and equipment related readiness are also being assessed. At the current time, Spartan trucks and engines, most Hale Pumps and LTI ladder mechanisms have been determined to be either unaffected by Y2K or are Y2K ready. This represents the vast majority of the Fire Department's apparatus fleet. Vehicles not in this group consist mostly of apparatus which is not regularly in service. Those vehicles are now being assessed.

Ambulance engines, transmissions and chassis are also not affected or have been reported by their manufacturers as being Y2K compliant. All defibrillators and pulse oxymeters have been assessed. Most of the department's defibrillators required remediation in the form of software patches. The San Francisco General Hospital Biomedical Engineering Department has completed the remediation of these devices, and they have been returned to service.

The Automatic Vehicle Location System, which provides the location of ambulances to central dispatch, is not Y2K compliant. The Y2K non-compliance will not cause the system to stop reporting ambulance location, but makes the date and time stamp of the report inaccurate. SFFD and DTIS are working with the system's vendor to correct this problem. The target completion date for this project is August 30, 1999.

Finally, all of the SFFD generators have been inventoried and are reported by the Department of Public Works to be Y2K ready.

The SFFD has also begun its contingency planning. An internal contingency planning committee composed primarily of officers at the Assistant Chief rank and above has been formed and is meeting approximately every two weeks. Contingency planning addresses both technical Y2K issues and special considerations raised by Millennium events that will take place in San Francisco on New Year's Eve. Among other things, the Fire Department will be contacting the owners and/or managers of San Francisco's 350 high-rise buildings to ensure that building management has assessed elevators and other devices which, if malfunctioning, would significantly impact the number of calls received by the SFFD.

Department of Human Services

The Department of Human Services (DHS) has identified the following services as mission-critical:

Protective Services

Welfare to Work

Eligibility Determination and Benefits Issuance

Homeless Services

Disaster Response Services

The Department of Human Services has made substantial progress in preparing for the year 2000. Inventory, assessment, and testing of all mission-critical systems is complete, and most are reported by the department to be year 2000 ready.

All of the mission-critical information systems are currently reported by the Department as either being year 2000 ready, or in the remediation phase. The Welfare Case Data System supports Medi-Cal and Food Stamps eligibility determination, cash assistance, and welfare-to-work services. It also maintains client indices for two adult social services programs. This system has been certified as Y2K compliant by its vendor, EDS. Additionally, DHS and DTIS have performed independent mainframe testing and will test again in August to ensure any add-ons or updates do not adversely affect performance.

The Case Management Information and Payroll System (CMIPS) supports the In-Home Supportive Services program. DHS runs an emulation program of this system, while the main system is run and maintained by the State of California. The State successfully converted to an upgraded Y2K compliant CMIPS program in late July, and it will be in full production statewide effective August 2nd. DHS has successfully tested its emulation program in a test region of the new program and began testing in the production environment on July 29th.

The Child Welfare System (CWS) which supports child protective services has been certified as Y2K compliant by its vendor, IBM, and by the State's Health and Welfare Data Center.

DHS has also completed inventory, assessment, and testing of its PC based local area networks and wide area networks. Remediation, which involves installation of patches on each PC, is 80% complete. The department has organized its compliance information and has entered its data into the Tracker 2000 database.

DHS has also completed its facilities inventory and has entered that information into the Tracker 2000 database. Independent verification and validation of facilities work has been done. It has been confirmed that the facilities assessment was thorough and that all necessary documentation is in place.

Finally, DHS has prepared a core outline to address its contingency planning needs. DHS' Information Technology and Facilities staff began meeting with PMO staff in early July to ensure that programmatic requirements are built into DHS contingency plans. It is anticipated that planning and documentation will be completed by the end of August for each mission-critical area, the core processes of those areas and the tools that support them.

Municipal Railway

The Municipal Railway has identified the following services as mission-critical:

Diesel Bus Service
Electric Trolley Bus Service
Light Rail Vehicle
Cable Car Service
Motive Power
Central Control
Paratransit Transportation

The Municipal Railway has been actively preparing for the Year 2000. Inventory and assessment of mission-critical systems is wrapping up with final auditing by the PMO. The Municipal Railway is testing major mission-critical systems that could have significant impacts on service to assure that they are Y2K ready. These systems include:

- **ATCS Subway Train Control System**: Testing is well in progress. No Y2K issues found to date.
- **LRV2 Streetcar**: Vendor certified system is Y2K compliant – testing scheduled for the first week of August.
- **Weekend Revenue Subway Test**: Full day test of subway ATCS system and LRV2 streetcar with date roll over scheduled for late August.
- **Electric Trolley Coach**: Testing complete –system is Y2K compliant.
- **Remote System Controls for Subway Extension and Embarcadero Extension**: Ventilation, security and ticket machine monitoring – testing is in progress.
- **Electric Power System Control**: Power monitoring and control of power substations. Awaiting vendor system upgrade and testing. Work around in place if required.
- **Surface Train Control Systems (2)**: Vendor certified – testing scheduled for mid-August.
- **Bus Maintenance Garage at Flynn**: Inventoried and assessed. No Y2K issues found.
- **Municipal Railway Radio System**: No Y2K issues found to date.
- **Diesel Busses**: Busses will run. No Y2K issues found.

The diesel bus fleet will be the primary mode of service in the event of power outages or power brown outs. All mission-critical systems supporting this mode have been evaluated for Y2K exposure. Plans are being developed to top off fuel tanks daily prior to December 31, 1999 and to secure additional temporary tanks and fuel.

The Municipal Railway has developed draft contingency plans and is currently refining and fine-tuning them. The plans identify key personnel, additional equipment and resources, establish roles and responsibility and include such detail as utilizing electric vehicle resources (operators, mechanics, road crews, etc.) to provide support and relief to Diesel Operations in the event of power outages.

Department of Parking and Traffic

The Department of Parking and Traffic has identified the following as mission-critical:

Traffic Signaling

Parking/Traffic Control

Parking Garages

Traffic Signaling

Parking and Traffic reports that date-sensitive traffic signal equipment is limited to traffic signal controllers and master system clocks. Non-compliant chips have been replaced. The new signaling system chips were tested by the manufacturer and determined to be compliant. In addition, Parking and Traffic has conducted in-shop testing on representative samples of this equipment to confirm Y2K readiness. Currently, signal status is being independently assessed and validated by the PMO.

Parking/Traffic Control

Parking and Traffic reports that their new radio communication system is currently in the process of being upgraded to the new 800MHz system. Implementation is scheduled for August 1999. Vehicles used to monitor City parking and traffic control issues have been determined by Central Shops to be Y2K compliant. These vehicles include Cushmans, Interceptors, Metros, and Trackers. Towing vehicles and equipment are provided through an outside contractor. This contract expired at the end of May and is being administered on a month to month basis until the new contract is awarded. The new contract will be certified by the end of the year and contains Y2K compliance language.

Parking Garages

Garages have been assessed as of May 31, 1999. Parking and Traffic's primary concern is with the emergency systems at these garages. Parking and Traffic reports that one fire and security system requires replacement. Replacement costs are in our new fiscal budget and the work is targeted to be completed by October 1, 1999. All other emergency systems, including elevator monitoring and backup systems and communication systems are reported Y2K ready. Secondarily, Parking and Traffic is concerned with the systems that control access to the garage and those which provide revenue control and collection. About half of the garages have been determined to have non-compliant parking access and revenue control systems. These non-compliant systems are scheduled for upgrades by October 1, 1999. In addition, manual work arounds have been developed to ensure that citizens will have parking garage access.

Police Department

The Police Department has identified the following services as mission-critical:

Vehicles

Communications

911

Facilities

Vehicles

The San Francisco Police Department uses three categories of vehicles: automobiles, motorcycles and specialty vehicles. The Y2K readiness of these vehicles has been assessed by the City and County's Purchasing Department, which has collected documentation indicating that the standard equipment in SFPD Patrol cars will be unaffected by Y2K problems. Add on equipment such as computers and radio equipment are being separately assessed.

The SFPD uses both Kawasaki 1000 and Harley Davidson FLH Police motorcycles. Both manufacturers have provided the SFPD with statements certifying that the motorcycles do not use date-sensitive chips and are therefore Y2K ready. As with vehicles, add on equipment is being assessed separately. The Y2K readiness of specialty vehicles is being assessed on a case-by-case basis.

Communications/911

The SFPD uses both radio and data communications equipment. This equipment, which includes the 911 system, is maintained by the Department of Telecommunications and Information Services and is covered in that department's section of this report.

Facilities

All SFPD buildings have been inventoried for the purpose of identifying and assessing any embedded systems which might be affected by the Y2K change over. These systems are maintained by the Department of Public Works, which is currently assessing them for Y2K compliance. Remediation and testing will be handled by the Department of Public Works.

Department of Public Health

The Department of Public Health (DPH) has identified the following services as mission-critical:

Inpatient Care
Emergency Care
Outpatient Care
Long Term Care
Mental Health Services
Jail Medical Facilities
Biomedical Devices
Hazardous Materials
Community-wide Emergency Response

The Department of Public Health has devoted substantial energy and resources to identifying and correcting Y2K problems. A department-wide committee of more than 30 individuals headed by Chief Financial Officer, Monique Zmuda, has been coordinating DPH's efforts.

The Department of Public Health has completed an inventory and assessment of all items potentially impacted by Y2K. Of the 12,000 items compiled in the DPH Y2K database, most were found to be unaffected by the Y2K date change. The remaining items have been prioritized for assessment and remediation according to their criticality.

Remediation

Remediation of all affected workstations is well underway and replacement of all impacted personal computers will be completed by September 1999. All network devices, including routers, switches and hubs have been assessed and updates are currently underway. All Novell NetWare operating system patches have been applied, and testing of all Novell servers is expected to be completed by August 1999.

All major information systems supporting patient care have been assessed. These systems are now either compliant or in remediation and testing. All major patient care systems, including the SMS suite of products used by the Community Health Network have been certified to be Y2K compliant. All other remediation is expected to be completed by August 31, 1999, with the exception of the Mental Health and Substance Abuse billing system, which will be remediated when a new, Y2K ready software version is released in September 1999.

Testing

Year 2000 date advance testing is being done on equipment and applications. The first test date was on May 14, 1999 and included 14% of the Department's hardware and operating systems, primarily NT servers. The second test occurred on July 24, 1999 and included 61% of all hardware and operating systems and applications running on these systems. In September 1999, the Department will date advance test 100% of its hardware and operating systems.

Initial results of the first date advance have been positive, with no significant data advance problems found. All major systems operated in the millennium without loss of data or power. The testing also provided the opportunity for MIS engineers to develop protocols for back-up, recovery and testing.

Facilities and Biomedical Devices

In December 1998, all biomedical and facilities equipment was prioritized as critical, significant or insignificant. As of April 1999, all critical systems for which DPH has primary responsibility were either Y2K ready or had the necessary resources assigned to become Y2K ready by August 31, 1999.

Over 7300 biomedical devices have been reviewed for Y2K compliance. Less than 10% were found to be date-sensitive. Of those that are date-sensitive, approximately 120 devices (consisting of 16 different types) were found to be non-compliant. The majority of these devices have now been remediated. It should be noted that the vast majority of these medical devices have manual work-arounds which would be implemented should any device fail.

Among the major biomedical items found non-compliant, the WatchChild fetal monitoring system requires a software patch that will be installed by August 31, 1999 and the Central Consoles in the intensive care and emergency units have been replaced. All work is expected to be completed by September 1999.

Telecommunications

DPH relies on Department of Telecommunications and Information Services (DTIS) for their telecommunications needs, and some telecommunications components have required multiple upgrades. DPH is actively working with DTIS to ensure that all necessary telecommunications upgrades are completed in a timely manner. A few remaining voice mail systems at a handful of sites remain to be upgraded and brought into compliance. These upgrades are currently in progress.

Hazardous Materials

DPH's hazardous materials unit will assess high risk users and formulate a strategy for ensuring that these users are aware of potential Y2K issues at their sites. The Hazardous Materials unit is also distributing a State Office of Emergency Services checklist to obtain information on the Y2K readiness of establishments that it regulates, and to assist those entities in achieving Y2K readiness. Additionally, the hazardous materials unit expects to conduct inspection of sites considered high risk before the end of 1999.

Automated systems supporting the Hazardous Materials unit have been upgraded and tested and are Y2K ready.

Supplies and Distribution
Major vendors for the Health Department's medical supplies and pharmaceuticals have been cooperative in sharing the Y2K plans. The two major suppliers, Allied Medical and Novation have active Y2K plans for maintenance of their production and distribution. Additionally, suppliers are working with California health systems, including DPH, to prevent overstocking and stockpiling which would adversely affect the vendor's ability to meet the needs of their clients.

Millennium Event and Contingency Planning
Finally, the Department of Public Health is actively working with the Office of Emergency Services (OES) on contingency planning for the Millennium weekend, and a department- wide subcommittee has been formed to address all issues, including increased staffing and medical coverage needs. DPH will continue to work with the Office of Emergency Services, the Fire Department and other agencies in coordinating health and safety procedures for the Millennium weekend period.

Additionally, all mission-critical systems have existing, documented manual back-ups, which can be implemented in the case of any unanticipated failures.

Public Utilities Commission

The City Department primarily involved with utility issues is the San Francisco Public Utilities Commission (SFPUC). The SFPUC Y2K compliance program started more than a year ago. That effort has included reviewing the compliance status of the SFPUC's software, hardware and equipment employing embedded computer chips that operate the potable water, hydropower, wastewater and administrative systems.

The SFPUC has identified the following services as mission-critical:

Water Distribution- Pipes, pump stations, reservoirs, quality monitoring
Water Treatment- Pumping facilities, process control and monitoring
Wastewater Collection- Pumping facilities, telemetry, monitoring
Wastewater Treatment- Pumping facilities, process control and monitoring
Power Generation- Hydroelectric facilities, reservoirs
Power Distribution- Transmission lines, substations

The SFPUC has devoted substantial energy and resources to identifying and correcting Y2K problems. Over 3,600 individual equipment items have been inventoried. A thorough assessment of mission-critical systems has revealed a limited number of items requiring remediation.

Remediation actions to address non-compliant equipment are underway. Remediation is taking the form of upgrading, replacement, retiring and workarounds. SFPUC plans to complete and test all identified remediation in advance of December 1999.

The inherent reliance of SFPUC's water and wastewater systems on gravity supports multiple back-up operating options which have been identified to mitigate the consequences of a variety of failure scenarios to citizen health and safety. SFPUC has focused a significant portion of its efforts in developing contingency plans to mitigate both unanticipated internal problems and potential external failures. Completion of Contingency Plans is targeted for September 1999. A set of exercises is being planned during September to ensure Y2K readiness and delivery of SFPUC mission-critical services.

SFPUC also delivers wholesale water to agencies throughout the greater Bay Area. SFPUC's Y2K efforts address water delivery to its wholesale customers at the same level of service as for its customers in the City.

In its capacity as the City's liaison with PG&E. SFPUC is working to prioritize power restoration and to ensure that mission-critical City services receive the highest priority in power distribution.

Department of Public Works

The Department of Public Works (DPW) has identified the following services as mission-critical:

Operation of Buildings and Facilities maintained by the Bureau of Building Repair

Emergency and Disaster Response

Street maintenance and Repair

Bureau of Building Repair (BBR) Operation and Maintenance of Buildings

DPW is responsible for the maintenance of the Fire Department generators and transfer switches. BBR is also responsible for the following facilities: Police Departments, Hall of Justice, the Youth Guidance Center, Trial Courts at McAllister and Polk St., the Emergency Communications Department/Office of Emergency Services on Turk St., and BBR's Caesar Chavez Street Maintenance Shop.

DPW-BBR reports that it has completed inventory and assessment of the Fire Department generators and, based on manufacturer compliance statements, has determined they are Y2K ready. Testing of these generators will be completed by October 1, 1999.

Additionally, DPW reports that it has completed inventory of Police Department facilities and all other facilities for which it has responsibility. DPW is working on assessment of facility life-safety systems and is identifying areas where upgrades are necessary. Manufacturer compliance statements are on file.

Remediation is in progress on building management systems software at Taraval, Mission, Northern and Bayview police stations. This work is expected to be completed by September 1, 1999 and testing will be completed by October 1, 1999. Additionally, DPW plans to test mission-critical items such as generators, as well as systems/devices for which it has not been able to confirm Y2K readiness by September 1, 1999.

Emergency and Disaster Response

DPW's role in Emergency and Disaster Response and exposure to potential Y2K issues is in staff mobilization. The primary potential for exposure to Y2K problems would exist with vehicles and radio communications. DTIS has responsibility for radio Y2K compliance and has notified DPW that its radios are compliant. Specialty vehicles are being inventoried and a list will be submitted to Central Shops for assessment.

Street Maintenance and Repair
Like Emergency and Disaster Response, Street Maintenance and Repair is a supporting function. DPW's Y2K exposure for street maintenance and repair is limited to vehicles and radio communications. See discussion above for the status of that equipment.

Purchasing Department

The Department of Purchasing has identified the following services as mission-critical:

Vehicle Maintenance and Repair

Vehicle Fueling

Machine Shop Services

Purchase/Procurement of Goods/Services

OES Logistics Support

Vehicle Maintenance and Repair

The manufacturers of City owned vehicles with embedded chips which are maintained by the Purchasing Department 's Central Shop have issued representations that their products do not have Y2K issues and that the chips embedded in standard vehicles are not date-sensitive. They have stated that the Y2K transition will not affect the safety or performance of their standard vehicles and they expect their vehicles will function normally into the new millennium. Consequently, Purchasing is assisting other City departments to identify their standard vehicles which have been outfitted with additional equipment that may require Y2K assessment. Radio and telecommunications equipment are examples of typical add-ons which require Y2K assessment. Once these vehicles are identified, the owning department is responsible for assessing any add on equipment.

Vehicle Fueling

Purchasing reports that inventory is complete for four of its City fueling stations. Assessment has been completed for the fueling stations at Central Shops, Golden Gate Park Maintenance Yard, DPW Corporation Yard and the Hall of Justice. The fueling system vendors have reported that their systems are compliant. The Y2K PMO is scheduling independent verification of the completeness and accuracy of the inventory and assessment. The Purchasing Department is working in conjunction with the Office of Emergency Services and the City's fuel contractors to ensure adequate supplies will be available for essential services.

Machine Shop Services

The machine shop and maintenance facilities (Central Shops) are reported to have no embedded systems and hence no Y2K issues.

Purchase/Procurement of Goods/Services

Purchasing tested compliance of ADPICS, its procurement and payment applications, and found minor Y2K related problems. The software vendor is providing corrections and Purchasing expects them to be in place by September 1999. Existing contingency plans will be invoked in the event of a Y2K related failure.

OES Logistics Support
In support of OES, Purchasing's emergency operating procedures provide for the immediate procurement of goods and services.

Department of Real Estate

The Department of Real Estate (DRE) has identified the following service as mission-critical:

Leased Facility Management

The Department of Real Estate has mailed letters to 48 building owners regarding life safety issues at facilities leased by the City and County of San Francisco. Only 13 responses were received. These responses are being evaluated by DRE with assistance from the City Attorney's Office. DRE is now contacting those building owners who failed to respond, or whose responses were inadequate, by telephone. DRE is aware that as a lessee, its rights may be limited. However, if legally permissible, DRE may seek to arrange independent engineering assessments of their buildings.

By August 15, 1999, DRE expects to have compiled sufficient information about all its leased buildings to allow it to determine what further steps are necessary to determine Y2K readiness.

DRE's assessment of City owned buildings at 25 Van Ness and 1660 Mission Street is complete and both buildings are Y2K ready.

Sheriff's Department

The Sheriff's Department has identified the following services as mission-critical:

County Jails: Intake / Release / Housing
Inmate Transportation
Security Services: City Hall / Courts / CAD 911
Emergency Response

The San Francisco Sheriff's Department (SFSD) is responsible for all functions associated with the intake, custody and release of inmates at the County Jails. Booking, warrant checks, and property storage and return are included in the Department's mission-critical functions. The booking and release functions are supported by the SFPD for ID processing and DPH for medical screening.

The Sheriff's Department maintains an Inmate Tracking System, which includes booking arrests into the jails. This system, Court Management System (CMS), is maintained by DTIS. DTIS has completed remediation of this system and it is now compliant. Contingency planning, in the event of unforeseen failures, is being carried out in conjunction with the other public protection departments. Should these systems fail, manual work-arounds, which are currently used when mass arrests occur, will be implemented.

Stored property is physically maintained in an electromechanical storage system. This system is being assessed by the PMO.

The central warrant function, which includes warrant entry and processing, is accomplished through access to local, state, national and international databases which are not maintained by the SFSD. The SFSD owns 12 personal computers associated with this system, which the department has assessed as being Y2K ready.

The SFSD houses inmates in six main county jails. County Jails 1,2,3,7,8 and 9 have been inventoried and assessed. The physical plants at County Jails 1 and 2 in the Hall of Justice are maintained by DPW. The other four jails are maintained by SFSD. The PMO is independently verifying and validating the jails most critical systems. All jail doors, which rely on power, have been assessed by the Sheriff's department to be Y2K ready. Additionally, jail locks have key overrides. Each facility is equipped with emergency back-up generators for power.

The SFSD uses a multitude of systems to ensure security at the Courts, City Hall and CAD 911. Other departments, including the Department of Public Works, DTIS and City Hall's Administrative Services, maintain these systems. The SFSD does maintain a few "stand alone" security systems, such as metal detectors, which are currently being assessed.

The SFSD's response to emergency situations is dependent on its vehicles, radio and data communication. DTIS maintains the radio communication equipment and is currently assessing, remediating and testing that equipment. The SFSD uses three types of vehicles: automobiles, vans and buses. According to the Purchasing Department's assessment, the mission-critical vehicles of the SFSD are Y2K ready. Any additional equipment (lights, sirens etc.) are currently being inventoried and assessed by the department. The radios and computers in these vehicles are the responsibility of DTIS and have been certified as compliant.

Department of Telecommunications and Information Services (DTIS)

DTIS provides information technology and communications services to City departments; this includes voice and data communications and a variety of computer based services. Computer services consist of enterprise and mid-range servers which run departmental business applications, and data networks which provides access between departments and their applications at the DTIS data center.

Communication services consist of voice and data communications supplied by vendors such as Pacific Bell and AT&T, City owned equipment such as PBX's and voice-mail systems, and a variety of related equipment. Pagers, cell phones, and radio communications systems are also the responsibility of DTIS and fall into this category.

DTIS has identified the following services as mission-critical:

Enterprise Computing Services

Computer Applications

Telecommunication Services

DTIS has provided the following status for each of their mission-critical services:

Enterprise Computing Services
Within the computer services arena, the computers, system software, and associated equipment have been inventoried, assessed for compliance, and remediated (completed). Testing to validate compliance is also complete. Contingency planning is underway and is targeted for completion by September 1999. As part of DTIS's disaster recovery plan, the Department conducts regular tests of an emergency backup facility ("hot site") at which the Department can restore mainframe operations. DTIS plans an August, 1999 test of this capability.

The data center facility is in a leased facility and the compliance status of emergency power, HVAC, and other facility components is currently being investigated. This work is approximately 90% completed.

Computer Applications
A number of the computer applications that are maintained by DTIS are defined as mission-critical or have a significant impact on the ability of the City to conduct its business. Mission-critical systems include Interim-911 Emergency Dispatch, police and other criminal justice applications, and the Case Data System for the Department of Human Services. Some of these systems are vendor-packaged software and are

represented to be compliant by their vendors; others are currently being remediated with the majority of remediation complete. All applications, regardless of vendor claims of compliance, are being tested to validate compliance status. Testing will continue through the calendar year.

Other significant City computer applications maintained by DTIS include payroll, general ledger (FAMIS), budget (BPREP), and procurement (ADPICS). Compliant versions of these systems have been installed and verification testing is underway b DTIS and its clients.

Telecommunication Services
DTIS is responsible for most all phone services for the City; a few enterprise departments, such as the San Francisco International Airport, have independent relationships and contracts. The City's primary vendor, Pacific-Bell, states that its facilities and all data and voice circuits serving the City are compliant. City owned phone switches and voice mail systems have been inventoried and assessed, and non-compliant switches have been upgraded to compliant versions. A small number of voice mail components are non-compliant and upgrades are in progress.

DTIS is responsible for all cellular phone services and cellular phones acquired through DTIS. Cellular-One, which is the primary provider of cellular phone service tc the City, has stated that its services are compliant. Multiple vendors provide the cellular telephones themselves. Over 90% of the phones that are in use by City departments are known to be compliant. A plan is being developed so that departments can seek compliance information from DTIS regarding models that are not known to be compliant. DTIS will facilitate replacement of models when compliance cannot be verified. A small number of phones are in use that have not been acquired through DTIS. Although DTIS is not responsible for these, the Department will offer replacement phones if requested.

DTIS is responsible for City paging services. A new contract for paging services and pagers is being negotiated. It is estimated that the new contract will be in place by September. The new contract may require departments to replace some pagers. DTIS will ensure that replacement pagers are Y2K compliant and will help departments ensure compliance of pagers currently in use.

DTIS maintains radio communications for voice and data transmission. Multiple City departments use these services. The inventory and assessment of all radio equipment has been completed. A small number of components have been found to be non-compliant and remediation is in progress for these. The radios themselves that are in use by Fire and Police departments have been found to be compliant. As with cellular phones other departments may determine, with DTIS assistance, that particular models are compliant or have them replaced with compliant models.

Wide Area Network Communications is the responsibility of DTIS. This consists of data circuits that connect most City departments to a single wide area network (WAN). This WAN is the means by which departments access centralized applications at the data center, communicate with each other via email, and have access to the Internet. DTIS is responsible for the overall infrastructure up to and including the departmental routers. Within the department each department is responsible for it components, generally consisting of Local Area Networks, servers, and desktop personal computers. The primary WAN components have been inventoried, assessed, and where needed remediated. A small number of peripheral components that reside on this network are still being assessed or have upgrades pending.

[redacted]

Mr. HORN. Let me ask some general questions for the panel as a whole. I've long felt since I got into this in 1996 that this is a management problem, not just a technological problem, and I'd sort of like to know from you now that you've been through this process, what are the management principles you followed that you think, for those that haven't really become involved in this, you could give them a little guidance?

So let's just go right down the line. I think I'm going to let you pass, Mr. Willemssen. Let's have your colleague there, Mr. Burton, from the city of San Jose. What's the management approach you've taken and where responsibility is being placed and so forth?

Mr. BURTON. I think the No. 1 issue has been awareness, and that's for managers throughout the organization to be aware. Whether or not it's from a standpoint of the general issue of the year 2000 preparedness or the individual services and key equipment items, to ensure that they are year 2000 compliant. It's, I think, self-realization you have to begin with, and if you're in denial, you certainly wouldn't begin addressing the problem.

Mr. HORN. Mr. Drysdale.

Mr. DRYSDALE. Our management approach is based on communication, participation and involvement by really everybody. So when I mentioned that our executives participated in the test, that was true. We were all there on Saturday working on it, and the same thing is true of our staff. We work together as a team. So primarily involvement, participation, continued good communications, we try to practice every day at work. That's just a common approach.

Mr. HORN. Mr. Garratt.

Mr. GARRATT. I think the fact that I have been assigned as the Y2K project coordinator from the city manager's office rather than a chief information officer is indicative of the visibility the council and the city management chose to give this issue. We have departments who have been working in very rigorous ways to solve their individual proprietary situations, but it does require a certain level of oversight and coordination and a constant message that enough is never quite enough. And that's the approach we've taken.

Mr. HORN. Ms. Hayashi.

Ms. HAYASHI. In the city of San Francisco which is a fairly decentralized city, the multiple programs primarily take responsibility for all their own operations. It was an important step in the Y2K effort to create a central, city-wide organization that existed to help coordinate the efforts between the departments, coordinate the communications about the interdependencies between departments, because a lot of departments that rely on the phone services, for example, are dependent on another city department for providing those services. Also for centralizing some of the issues to avoid duplication of work, and directing resources also, because as we've seen departments that perhaps don't have enough resources in their own pockets, that we could direct some personnel and some expertise to them so that they can get the job accomplished quickly.

So the central oversight has been critically important, and I think I agree with the message of motivation as well, that everybody needs to keep working as hard as they can.

Mr. HORN. Since we have three cities on this panel, San Francisco, Santa Clara and San Jose, I'm curious if any of you have had the type of exercise that Rockville, MD and Lubbock, TX ran through where they advanced the date forward, in a department in the middle of the night and then see what happens to your emergency coordination operation. Has any of you done that at this point, or have we just dealt individually with adaptation of codes?

Ms. HAYASHI. That has been done in San Francisco, but again, many of these year 2000 readiness preparations were done on a department-by-department basis. So we haven't had a city-wide exercise, but there has been a lot of date simulation testing in individual departments.

Mr. HORN. Because certainly when you have department responsibility, the question is do they have connection with other departments to get their job done?

Ms. HAYASHI. Exactly. And that's why the central program management office is the grease that keeps those wheels moving.

Mr. GARRATT. I have heard the Rockville staffers and the Lubbock staffers explain the exercise they went through. We have not attempted to perform something like that. We pushed certain systems beyond the millennium. We had the unique experience in one system where it went beyond and operated, but it was very difficult to pull it back. And there was a bug in the software from that perspective. But we've been fairly limited and judicious on pushing these systems as a unit.

Mr. BURTON. In the city of San Jose we have pushed the date forward on our network, our city-wide network, to the year 2000 and exercised the system. I believe that was back in March, and have a plan to do that again in September over the Labor Day weekend. In addition, for our computer clusters for applications we have tested systems with the system dates rolled forward, as well as the individual applications, flexing them with functionality in the next century. Our first test in that was in the month of May this year. We actually have a test underway today in our computer center with a date rolled forward to the year 2000. We also have one scheduled for August 28th and again on Labor Day, as I mentioned.

Mr. HORN. Some have mentioned over the last few years that there are some additional dates we need to be concerned with, and your comment on September, I thought I'd use that, September 9, 1999 bothers some people as it might mess up some computers because that apparently was used as a symbol for a number of computer programs in the past, and the other being the fact that we have a little extra day in February 2000.

Does any of that concern you one way or the other?

Mr. BURTON. We identified 19 key high-risk dates potentially. The high risk dates have been examined against the application to find out what dates that application would have at risk. Our testing plan includes flexing a minimum of two of those dates for applications: most assuredly the roll over as well as leap day, and then identification of some other date. For instance, not only do you face January 1st and leap day, but with remediated code, et cetera, we're concerned about month end closes, quarterly closes, fiscal year closes and calendar year closes in these remediated applications. So there are quit a few dates that we're looking at.

Mr. HORN. Mr. Garratt, any thoughts on that?

Mr. GARRATT. As I mentioned in my presentation, we've replaced a good number of our systems with object-oriented programming languages, C++, that deal with the year as a four-digit equation. Our finance system has been remediated, and we are aware, and we will be watching very carefully certainly on September 9th. The programmers have looked into the system to make a determination if that could be a problem. They did not believe it will be a problem.

Mr. HORN. That's very interesting, and I wonder how about San Francisco? Have you done that?

Ms. HAYASHI. Yes, yes. Leap year and other potentially sensitive dates are a part of what we have taken into consideration in examining the IT systems.

Mr. HORN. Mr. Drysdale, you've given us very helpful information on the water, and as understand it, there are 200,000 public water systems regulated under the Safe Drinking Water Act that serve about 240 million people in our country. The remaining population obtains most of their drinking water from private wells. So I'm curious, is the San Jose Water Co. ready for January 1, 2000, to ensure that there are no violations associated with the Safe Drinking Water Act?

Mr. DRYSDALE. Yes, Chairman Horn, our water quality staff is part of the group that would be available that evening. But typically, our staff that works around the clock monitors for different types of matter that can be in water that might indicate a violation of the Safe Drinking Water Act. Generally, when the water is tested here in the valley for all the required different types of chemicals and matter that can be in the water, typically we have nondetectable traces. It's not possible to detect anything that would be required by current regulations. So as far as wells, private wells, here in town are, the oversight for that is the Santa Clara Valley Water District. So we work with them as far as monitoring our own wells, but private wells, we don't have that responsibility.

Mr. HORN. Does the Santa Clara Valley Water District include all of southern Santa Clara County? How does that work?

Mr. DRYSDALE. Yes, it does. In general, that would be a fair description of their service area.

Mr. HORN. That includes the Pajaro River, which is a river on the southern end of the county, marks the border.

Mr. DRYSDALE. I believe it would.

Mr. HORN. I'm just curious, because you've mentioned Federal and State water that you have access to, which I assume is coming through the San Luis Reservoir, isn't it?

Mr. DRYSDALE. Yes, it is. There's San Luis Reservoir water, and there's also water that's directly piped into the valley to the two treatment plants that the district operates. One is on the east side of the valley, and one is on the west side of the valley.

Mr. HORN. Is there projected, given the population growth in San Jose and Santa Clara County, is it projected that it will have a very tight situation on water whether it be the year 2000 or not?

Mr. DRYSDALE. I'm not familiar with those projections, but I don't believe that there's a problem. I do attend some of the water retailer meetings with the district, and there's never been expressed any concern for that.

Mr. HORN. Now for the agricultural use where they do have wells on a number of these farms. What's been the water level? Has it been going down substantially in the last 20, 30 years?

Mr. DRYSDALE. No. On the contrary, with the use of import water, the primary supply for the valley ground water is at record levels.

Mr. HORN. Where do you touch the water supply? What's the footage digging a typical well?

Mr. DRYSDALE. Depends upon the usage, the nature of the soil, the nature of rock. There are different levels. But one very good example not far from here, we have a local highway that's about 15 or 18 feet below the surface level and water is percolating through that highway right now, and that's a problem that people are trying to deal with. So the water is typically quite high.

Mr. HORN. That's interesting. In Los Angeles what many of us know as the Century Freeway named after my predecessor, Glen Anderson, who chaired the Transportation Committee of the House, turns out they have exactly that problem, that water's coming up there, and the water replenishment agencies are now billing the State Highway Department for taking their water. It's having its amusing aspects, but it becomes very difficult when your freeway starts moving around. So that's happening here. That's fascinating.

Let me ask Mr. Willemssen who has gone through many panels, that raises good questions as his colleagues do in GAO.

Mr. WILLEMSSEN. One issue that was briefly touched upon by one or two of the witnesses that I would encourage all the organizations here to keep in mind is the value of independent verification and validation efforts, especially to the extent that you can publicize those efforts and let citizens know that another set of eyes has indeed gone in and taken a look at your most important systems and made judgments about their compliance status. That can go a long ways in further assuring citizens' readiness. That's one thing to keep in mind.

An additional item, and you touched on this in one of your questions, there are tremendous value in testing business continuity and contingency plans. There are things that come up during these test exercises that were never considered early on, so I would also encourage the organizations to consider that.

In addition, I believe the city of San Francisco representative mentioned the importance of communicating to the citizens during the rollover period. I believe the States and localities will be hearing much more from FEMA regional offices and from the executive branch on the plans of John Koskinen's information coordination center in this regard with their purpose of trying to get out reliable, consistent information to the public during the rollover period. The individuals here should be playing a role in that and will be getting further information on it.

Mr. HORN. Thank you. Any questions you'd like to ask of your colleagues now that you've heard all of this, and any questions we should have asked but didn't have the brains to ask, we'd like to take those questions too. So anybody have some additional thoughts after hearing the dialog?

OK. Everybody's satisfied there. Driving home to San Francisco you're not going to say, "Gee, I should have asked that"?

Ms. HAYASHI. I think we'll have other opportunities to talk to each other.

Mr. HORN. At midnight, January 1st?

Ms. HAYASHI. No. I think the interagency dialog has been very valuable, and everybody is taking advantage of it.

Mr. HORN. I should ask, where are you all going to be that night, January 1st? I assume you're in your command headquarters on water, electric and all the rest. Yeah.

Well, I'll be flying on a plane. We'll see what happens there. I've told the FAA Administrator don't upset the controllers that day, will you. Leave them alone.

Anyhow, thanks for coming. You've had very thorough things. There's some excellent work where people could be used either on bills or everything else to get the message over. I think we'll steal liberally from all of your ideas. Thank you.

Ms. HAYASHI. Please do.

Mr. HORN. OK. We're moving to panel two. Panel two consists of some of the key corporations in Silicon Valley as well as Pacific Bell and the San Jose International Airport. We'll be glad to fly in and out of. It's a fine airport.

We have Mr. Whitworth, Mr. Cavaney and Mr. Hall and Mr. Latino, Mr. Tonseth. I think that's it.

OK. Gentleman, if you raise your right hands.

[Witnesses affirmed.]

Mr. HORN. The clerk will note that all five have been affirmed, and we will begin with Mr. Whitworth. And as I mentioned earlier, you might not have been here, automatically that full statement of yours goes in the record. We'd like you to summarize it so we'll have more time for questions and answers and dialog, but we appreciate all of your hard work and thank you for coming.

Mr. Brad Whitworth is the Y2K marketing & communications manager for Hewlett Packard Co. We're glad to have you here, very distinguished name in computing.

STATEMENTS OF BRAD WHITWORTH, Y2K MARKETING AND COMMUNICATIONS MANAGER, HEWLETT PACKARD CO.; PAT CAVANEY, YEAR 2000 PROGRAM MANAGER, CUSTOMER SERVICE AND SUPPORT GROUP, HEWLETT PACKARD CO.; RICHARD HALL, DIRECTOR, CALIFORNIA GOVERNMENTAL AFFAIRS, YEAR 2000 PROGRAM MANAGER, INTEL CORP.; TOM LATINO, PRODUCT MANAGER, PACIFIC BELL; AND RALPH TONSETH, DIRECTOR OF AVIATION, SAN JOSE INTERNATIONAL AIRPORT

Mr. WHITWORTH. Good morning, Mr. Chairman. I am pleased to be with you today to talk about the year 2000 program at HP. The timing for my appearance really couldn't be better. We just passed an important internal milestone in HP's Y2K program that I'll tell you about in just a moment.

HP is a worldwide electronics company, yet we're here in Silicon Valley. 1998 revenues over $48 billion. We employ about 120,000 people and conduct business in more than 120 countries around the world. We are the second largest computer company in the world, the 14th largest company in the Fortune 500. Probably best known for LaserJet and InkJet printers, PCs and our high performance computer systems. We're also the maker of hand-held calculators for students, patient monitoring systems for intensive care nurses, gas chromatographs for chemists.

Y2K takes on three dimensions for us as an organization. First is that we had to make sure that the 36,000 products that we sell and ship today are all Y2K ready. Second, we want to make sure that customers who purchased products from HP in the past know the Y2K compliance status of their HP products and that they understand the need to check the readiness of HP gear in their own environment. And third, we're working hard to make sure that Y2K doesn't create any problems for our own operations. So we've been checking everything from orders processing systems in our Atlanta sales office to the electricity supplied to our Puerto Rican manufacturing facility to the phone system in our Beijing, China, operation.

I'll spend some time talking about the first and third points in our Y2K program on products and our own operations, and then my colleague, Pat Cavaney, will tell you about the ways we've been working with our customers around the world and how we're helping them prepare for the move to the next century.

Let me start with that third dimension to our Y2K program, our internal readiness. I mentioned we just passed an important milestone in our Y2K program. We had an internal readiness date of July 31st. We picked that date as the one by which we'd have all of our critical information technology systems and business processes ready for Y2K, and based on the reports from our managers around the world, we made it. In only a few instances do we still have some exceptions remaining, but we're confident that we'll be resolving those in the next few weeks.

Meeting that target date of July 31st was not a trivial matter for a company of our size and complexity. For example, it meant checking the Y2K readiness of 150,000 personal computers, another 24,000 computer workstations, about 8,500 critical business software applications, 300 PBX systems, 13,000 servers, 2,700 routers, and all of these located in HP offices in more than 50 countries. That means we also had to check with more than 110,000 suppliers all over the world. We rely upon them for about 600,000 parts that we use to manufacture our products. They provide us everything from microprocessors to monitors. We're generally satisfied with their readiness programs.

However, the complexity of that supply chain and that chain's reliance on a global network of transportation providers to move raw materials subassemblies and finished products does represent HP's largest Y2K vulnerability. This is particularly true outside the United States where we've discovered, as have Y2K experts like the Gartner Group, some countries have been late in addressing Y2K. So we're working closely with all these suppliers. But because many of these issues are beyond our direct control, we're spending a lot of time developing contingency and backup plans. I would certainly say that this is the area of focus for us for the rest of the year.

Now let me tell you about the HP products that I mentioned. When we launched our Y2K program, we needed to make sure that all of today's products were Y2K compliant. We also needed to work back through thousands of products we've delivered in prior years to determine if they're Y2K ready, and also we needed to put in place a process to make sure that all of our future product offerings are also ready for Y2K.

When we started a few years ago, there was no industrywide definition for year 2000 compliance, no testing standard. So we developed our own, based in part on GTE's Y2K test pattern that our IT organization had been using since 1996. We've been using it companywide ever since, and it's become a model in the industry to organizations like I–Triple E and NSTL, who developed their standards. Most important for us, it's now embedded as part of our ongoing test processes we use for every new product we introduce.

So where do we stand today with our products? Well, all of the products that we've introduced since July 1, 1998 are Y2K compliant, and almost half of 115,000 products in our compliance data base are fine with Y2K simply because they don't process dates at all. There are large families of some of our largest and most popular products where there are no Y2K problems. For example, our DeskJet printers, our scanners and all but early versions of one model of our LaserJet printer are all Y2K compliant. We do have some older products that are not Y2K compliant. Most of these non-compliant products have been obsolete for some time. They are no longer supported by HP.

However, we've made an important commitment to our customers on these older products. For every product that we've delivered since January 1, 1995, we will have a Y2K update or a replacement product available, and available at no additional charge if the product is covered under a support contract or warranty. One of the industry consultants who has studied our program calls this commitment to customers the most generous he's seen. But really, Y2K isn't about our policy or products or internal operations. Y2K is really about our customers and making sure that they have the information and the know how that they need to get their own computing environments ready for Y2K and continue their businesses.

So I'd like to ask Pat Cavaney to share with you some more details about our customer Y2K programs, and what we've done so far, and what we'll be doing in the months ahead.

[The prepared statement of Mr. Whitworth follows:]

House Committee on Government Reform
Subcommittee on Government Management, Information and Technology

Field Hearing
on the Efforts
of State and Local Governments
and Businesses to Address
the Year 2000 Computer Problem

Prepared statement from
Hewlett-Packard Company
Brad Whitworth, Y2K Marketing Manager

Saturday 14 August 1999
San Jose, California

Hewlett-Packard Company prepares for the Year 2000

Hewlett-Packard is a $48 billion technology company with more than 120,000 employees who conduct business in more than 130 countries. As the world's second largest computer vendor, we are committed to addressing the challenges of the rollover to the Year 2000 for our thousands of products and millions of customers around the world.

As the 14th largest company in the *Fortune* 500, HP must also address all the ways that Y2K affects our own operations – from computer and telecommunication systems to manufacturing to support to distribution activities. We expect to have spent about $250 million on all our internal readiness efforts over the duration of the Y2K program. Most of that expense covers internal information-technology improvements described later.

Hewlett-Packard has been hard at work on all fronts to achieve Y2K readiness. Based on feedback we've received from outside evaluators, journalists and industry analysts, we feel we have one of the best Y2K programs in our industry.

To coordinate the broad range of Y2K programs across the entire company, HP established a Year 2000 Program Office. The Y2K Program Office is the centralized team that coordinates the various efforts that have been under way since 1996 in many places around the company.

The leader of HP's Y2K Program is General Manager Bernard de Valence, a 21-year HP veteran with a wide range of prior company management experience. Based in Cupertino, California, Mr. de Valence is responsible for HP's overall Y2K programs, including all matters related to internal readiness, products and customers. He reports to HP's 8-person Executive Committee through Executive Vice

President and Chief Financial Officer Bob Wayman. Mr. de Valence provides progress reports to the company chairman, Lew Platt, and CEO, Carly Fiorina, to the company's presidents, and to the company's board of directors.

Hewlett-Packard is a large, decentralized organization in which decision-making is pushed to the lowest possible level within each business and geographic region. Each business – whether it's the Healthcare Solutions Group that makes defibrillators or the R&D team that develops personal computers for the home – is implementing its own specific Y2K program. These Y2K programs are linked by common processes and functions, but fine-tuned to the special needs of that business unit's customers, products and processes which that unit uses to conduct its business.

The individual programs are coordinated and monitored through the company's Y2K Program Office, a Y2K Board and a Y2K Council. The business-specific Y2K plans are visible to employees via internal web sites on the company's Intranet.

HP's plan to split into two companies – a computing and imaging company that will keep the HP name, and an instrumentation company (named Agilent Technologies) will have little effect on our Y2K efforts. We'll continue to have one Y2K program serving both companies, even after the split. The official split is expected to take place during the first half of calendar year 2000.

HP's Y2K product story

Today HP manufactures, sells and ships more than 36,000 different products – ranging from tiny light-emitting diodes to defibrillators to inkjet printers to computers. When we originally launched our Y2K program, we needed to make sure that all the HP products we are delivering today (and all those that we will ship in the future) are Y2K compliant. We also needed to work back through the thousands of products we've introduced in prior years to determine if they met HP's single, companywide compliance definition.

This challenge was further complicated by the fact that, when we started preparing for Y2K, no single Year 2000 compliance definition or testing standard existed anywhere in the industry for HP's wide range of products. That's why we decided to develop our rigorous "standard" for compliance testing. It was originally based on the GTE Y2K test profiles that had been contributed to the public domain and were put to use by HP's internal IT organization in 1996.

We completed our product compliance testing in mid-1998.
We evaluated more than 100,000 of our current and past products. And we continue that process to this day by evaluating all our new products that process dates. The results:

□ All HP products shipping today are Y2K compliant. (A very few products may require a customer action to make the product compliant.)

□ The Y2K compliance status for more than 100,000 current and past HP products is now available on our website at http://www.hp.com/year2000.

□ On the web site you'll discover that almost half (48 percent) of the products in the compliance database are NDRP – they do not process any date-related information – and are therefore considered compliant.

You'll also learn that there are large product categories where there are no Y2K problems – for example, our DeskJet printers, our scanners and all but early versions of one model of our LaserJet printers (the 3100) are all Y2K compliant.

In the case of some HP businesses, we have augmented our own definitions of compliance and compliance testing using independent test labs. For example, HP's lines of personal computers and network servers meet the standards of the National Software Testing Laboratory – the world's largest independent tester of PCs – and they go beyond those levels to pass HP's compliance standards as well.

HP's Y2K customer story

We want to make sure that customers who have purchased products from us know the Y2K compliance status of their HP products and that they are taking responsibility for checking the readiness of that equipment in their own environment.

We know who many of our customers are ... they purchased their HP products directly from us and many still rely on HP for servicing those products. However, there are many more who purchased HP products, including printers and personal computers, through any number of our dealers or distributors around the world. Unless those customers completed a warranty registration card or the on-line registration that comes with a new PC, we do not know who they are or where those pieces of equipment are located. (Fortunately, most of the products that people buy through dealers and channel partners do not present any Y2K hardware problems at all. That's true for all of HP's inkjet printers and all but one model of our LaserJet printers).

A key goal for HP is to reach as many customers as possible to make sure they to check the status of their HP equipment as well as the readiness of their entire IT environment.

Under the umbrella of the companywide effort to inform customers, each of HP's major business segments has initiated its own customer outreach program. Each of these programs is sponsored by its respective Y2K business manager and is managed in the customer-care segment of that business. For example, our Healthcare Solutions Group has mailed letters to its customers where we know that one of the products they've purchased from HP is not Y2K compliant. Our Computer Services and Support Group has mailed Y2K information to all its current customers on an HP support contract. In addition, our Enterprise Computing Sales organization has been scheduling Y2K meetings with many thousands of its largest customers around the world.

HP's Year 2000 program offices around the world respond to customers' requests for information about the Y2K readiness of any HP products. These groups of HP employees answer customers' letters, faxes, phone calls, surveys about Y2K.

We have also made sure that all HP call centers and response centers worldwide are adequately staffed and trained to handle Y2K questions. Each customer-interfacing organization has received training and has deployed Y2K specialists to help their organizations answer in-depth Y2K questions. HP's field organization has been equipped with the latest information on product compliance, services, upgrade programs and tools to assist customers with their Y2K readiness.

For customers who do not have access to the Internet and our website, HP's customer call centers and sales and support offices get answers to customers' Y2K inquiries.

HP's central Y2K web site has been active since early 1997 and is now attracting more than 250,000 visitors a month. That number has grown steadily since November 12, 1998, when we began providing customers with direct web access to our "compliance database" listing more than 100,000 current and past HP products. This database receives more than 140,000 visitors a month.

We are working hard to inform the millions of customers who are not on a current HP support contract about our Y2K efforts. We're including a Y2K message in every press release the company issues in 1999, in the annual report, in select advertisements and direct-mail campaigns in many countries, and in messages at key trade shows and conventions.

We have plans in place to increase our staffing to meet the expected increase in demand for customer support as we move into the New Year. Our customer support response centers will be open to provide Y2K assistance to customers over the rollover weekend. Barring any sort of life-threatening events or some sort of government-imposed priorities, our customers will be our top concern. All HP operations will give absolute priority to helping customers achieve their own business continuity.

At this point we haven't experienced any significant impact from Y2K on our sales, either positive or negative. We know that some industry observers foresee a slowdown in sales of large computer systems; others predict a surge in PC sales; some say service and support revenues are likely to increase. We're watching for any of these trends and at this point, we haven't seen any clear, direct impact of these on revenues.

HP's internal Y2K story

Besides helping customers prepare for Y2K, HP people are working hard to ensure that all of our own internal operations move smoothly into the next century. To do this, we have to look at everything: our information technology systems, our relationships with thousands of suppliers and contractors, and hundreds of facilities around the world and much more.

We were one of the first companies in the industry to tell our employees that they will be playing a key role in solving customers' Y2K issues toward the end of the year. In January of this year, we warned employees that, unlike prior years when we'd often closed between Christmas and New Year's, we expected them to be ready to help customers.

So now we're less than five months away from the end of the year. We've just passed our internal readiness date of July 31, 1999. As of that date, we have virtually all our critical internal systems, processes and operations ready for the Year 2000; we have business plans in place with contingencies to get beyond any glitches; and we will use the remaining months of the year to test and validate those plans. On the following pages you'll read about our internal readiness efforts with our information-technology programs, our manufacturing operations; our facilities and our suppliers.

Information Technology

Hewlett-Packard has built one of the largest information technology networks in the world today. Our computer systems – clients, servers and applications -- are found in HP operations around the world, run by corporate, regional and business management to meet their strategic needs. Here is a statistical overview of the complex operation we use to move data, voice and video around the company:

- Nearly 175,000 clients (149,000 personal computers and 24,000-plus HP-UX workstations) throughout the company
- More than 13,000 servers (7,700-plus HP-UX servers, 5,500-plus NT servers, 650-plus HP3000 servers)
- 30-plus terabytes of data transmitted on intranet each month via 2,700 routers
- more than 2,600 subnets and 325,000 IP devices on the intranet
- 55,000-plus employees who access HP systems remotely (working from customers' sites, from hotel rooms or from home)
- 141,000-plus e-mail subscribers who send 33 million e-mail messages each month
- 120,000 voicemail users on 195 voice-messaging systems
- 130,000 desk phones averaging more than 8 million calls each month
- 25,000 cellular phones averaging more than 5 million minutes of calls per month

Part of our job of preparing IT for the next century of computing was simplified because HP's internal systems moved entirely off of mainframe computers in 1996. As part of that initiative, several in-house developed applications were replaced with off-the-shelf software that was already Y2K compliant. HP's new human-resource (HR) systems are a case in point. We replaced our own internally developed information system with a version of the commercially available PeopleSoft® HR system that has been tailored to meet our specific needs.

HP has been addressing the Y2K issue across the entire IT spectrum for many years now, with a special emphasis on making certain that company-critical processes and their related software applications and hardware systems are made Y2K compliant before any others.

Early in 1996, the HP IT Year 2000 Initiative named Y2K the number-one priority for the worldwide Information Technology function. As part of this initiative, the company's Chief Information Officer (CIO) created a Year 2000 Coordination and Assistance Center (CAC). The CAC manager reports directly to CIO Mike Rose. The CAC is the coordinating body for HP's decentralized IT organization

In addition, HP IT established an Event Management Plan (EMP). With remediation now complete, IT's focus is now on protecting operations during the actual millennium change. Our success during this period will come from our contingency planning, testing those plans, and through Event Management Planning.

In March 1999, HP announced restrictions on new IT application releases and enhancements to existing applications or other infrastructure components. These restrictions enable HP to maintain a stable IT environment so that our systems can properly support our customer assistance processes.

Manufacturing, Distribution and Logistics

Hewlett-Packard currently markets more than 36,000 different products. Many are manufactured in a "made-to-order" style in one of HP's 59 manufacturing facilities around the world and sold by HP sales reps directly to customers. Some are built at HP facilities for broadscale distribution through dealers, distributors and large retail companies to customers. And, for an ever-increasing number of products and sub-assemblies, HP uses subcontractors in different parts of the world for our manufacturing processes

When the manufacture of these products is complete, the distribution of them presents an increasingly complex business challenge involving several levels of warehousing and shipping efforts. HP uses more than 900 different carriers and freight forwarders worldwide to handle this complex undertaking. In fairness, most of the transportation is handled by less than 50 firms. The company is also one of the top 10 ocean shippers in the world.

The Y2K strategies for manufacturing, distribution and logistics are all decided by HP's businesses, drawing upon the expertise in various corporate functions. In most cases, there are three levels of expertise at work on Y2K (and other) issues in manufacturing, distribution and logistics:

- Centralized (corporate, group or regional) functions
- Decentralized (division or local) functions
- Coordinating bodies (committees or councils)

For example, there is 55-person "corporate" logistics team that provides day-to-day leadership and coordination for the logistics function. There are hundreds more people who work in logistics organizations in HP factories, distribution facilities and country organizations around the world. And then there is a 22-person Logistics and Global Trade steering committee that manages the companywide policy, leads companywide initiatives, directs companywide information-technology programs to support logistics and helps leverage companywide purchasing power with key suppliers. The steering committee is made up of representatives from HP's business units, the major geographies, the corporate function and is supplemented by specialists in various forms of transportation advisors from related HP functions like government affairs.

Each HP business organization is responsible for making its own decisions about manufacturing strategies and maintaining its relationships with its suppliers and subcontractors. However, HP's Corporate Procurement team coordinates with many of the common suppliers on behalf of the entire company. So, for example, HP Procurement has been conducting end-to-end application testing with HP's top seven contract manufacturers. HP Procurement is assessing these manufacturers capability to conduct business prior to and beyond the Year 2000.

In January, the Logistics/Global Trade steering committee identified the primary international (air and sea) ports that are key to HP shipments. HP is working with specific freight forwarders to assess each port's Y2K readiness and define contingency plans for that port.

Facilities, Site Services and Business Operations

HP is committed to making sure its offices and manufacturing facilities are ready to support customers in the Year 2000. This is a big challenge because HP owns and leases properties all over the globe. The company owns manufacturing facilities in 28 U.S. cities, mostly in California, Colorado, the Northeast and the Pacific Northwest. The company also has its own research and manufacturing facilities located in 31 cities throughout Europe, Asia Pacific, Latin America and Canada.

HP's sales and support network is even more extensive. We sell our products and services through more than 500 of our own sales and support offices in more than 50 countries and a vast network of distributors and retail outlets that extends to another 80 countries around the world.

The Year 2000 initiative for the company's facilities is being managed by HP's Real Estate Facilities Operations. Each factory, distribution center and country organization has an assigned Y2K program manager responsible for ensuring Year 2000 readiness. In many cases the local Y2K program manager is working with the local procurement organization. In addition, every HP organization is expected to complete a Y2K internal readiness plan that 1) is coordinated with related HP business units and 2) provides contingencies that would be implemented if certain triggers occur.

Each quarter the status of all 573 HP facilities around the world and the status of their readiness programs are updated on the Facilities Operations internal web site.

Suppliers

Hewlett-Packard relies on a large number of companies around the world to provide materials, parts and services to our global operation. While many people think of suppliers simply in terms of providing raw materials, our definition at HP is much broader. Our suppliers provide everything from incoming parts to security services to contracted manufacturing to distribution.

Today, we have more than 600,000 "active" parts that are used to manufacture our products and we do business with more than 110,000 suppliers who are vital members of HP's supply chains.
Numbers of this magnitude make the Y2K challenge sound overwhelming. But making the job considerably simpler is the fact that most (more than two-thirds) of HP's total material buy comes from just 140 centrally managed suppliers and seven contract manufacturers.

HP's companywide procurement organization has implemented an extensive program for Year 2000 Supplier Readiness. One portion of the program is managed directly through the corporate procurement team at HP's headquarters in Palo Alto. The rest of the effort is managed using the same business process model by procurement teams in HP's business units and geographic operations around the globe.

HP completed an initial risk assessment in June 1998 in partnership with suppliers to assess overall business impact. HP's Year 2000 supplier program managers across the company coordinated with each critical supplier and completed a follow-up review and escalation plan. In some cases, to meet Y2K readiness, the company has replaced high-risk suppliers or eliminated suppliers from consideration for new business. New suppliers are assessed for Year 2000 compliance before being approved as a HP vendor. Contingency plans are finished and testing of these plans will continue through the rest of 1999.

All of the company's material-management systems have been migrated, tested and successfully implemented. Contract extensions and forecasts are being correctly processed.

Hewlett-Packard was one of the first companies in the high-tech industry to implement an Electronic Data Interchange (EDI) program. The program started in 1984 and now includes support and implementation services for 52 HP organizations and more than 800 suppliers and contract manufacturers around the globe.

To make sure that all of HP's EDI partners were ready for the rollover to the Year 2000, we contacted them to determine if their EDI data was fully integrated with their own business applications. HP and its corporate EDI suppliers completed all EDI migration by November 5, 1998. All joint testing was completed by the end of January 1999.

Conclusion

Meeting the challenge of Y2K is a complex job, particularly in an organization the size and diversity of Hewlett-Packard. Our range of products and the global nature of our business means that you'll find tens of thousands of HP people who have been solving Y2K problems. They're engineers who are making sure that your HP products won't create headaches for you in the next century. They're customer support specialists who have been answering your Y2K phone calls for the last couple of years. They're sales people who are working with their customers to make sure that they're ready for the new millennium.

We're committed to making the transition into the next century a successful one for our customers and for our company.

Questions?

If, after reading this testimony, you find you have more questions about HP's Y2K efforts, please visit our web site at:

http://www.hp.com/Year2000

or write, fax or phone us at:

Hewlett-Packard Company
Year 2000 Program Office
19111 Pruneridge Avenue, MS 44L17
Cupertino, CA 95014 USA
Phone: 1-408-447-6051
Fax: 1-408-447-2008

Brad Whitworth

Brad Whitworth is strategic communications and marketing manager for Hewlett-Packard's Year 2000 program, based in Cupertino, California. He is responsible for coordinating the external and internal communications efforts around Y2K. Brad joined HP in January 1980 and has served in a number of communications management and public affairs roles during his nearly 20 years with the high-tech company.

He holds bachelor's degrees in both journalism and speech from the University of Missouri and a master's degree in business administration from Santa Clara University.

Mr. CAVANEY. Good morning, Mr. Chairman. I appreciate the opportunity to speak with you today regarding Hewlett Packard and our approach to Y2K readiness in our role as a provider of customer support for our products. My name is Pat Cavaney, and I'm the year 2000 manager for Hewlett Packard's Customer Service and Support Group.

HP has employees and authorized distributors in 120 countries providing service and support all the way from homes to small businesses to large Fortune 500 corporations. Our goal is to help our customers achieve their own Y2K readiness. In his statement, my colleague mentioned the extensive products evaluation HP has performed on our current and past products and what we're doing to offer Y2K updates for our previously shipped products.

I'd now like to briefly address how HP has approached informing and supporting our customers through extensive proactive and communication efforts. This is the most far-reaching customer communication program that HP has ever undertaken. A key goal for HP is to reach as many customers as possible to make sure they check the status of their HP equipment as well as the readiness of their entire IT environment. Under the umbrella of the company-wide effort to inform customers, each of HP's major business segments has initiated a customer outreach program. Let me highlight a few of these for you.

Our customer support organization has mailed Y2K information to all of its current customers under a support contract and informed them of the compliant status of every product covered under a support agreement. Today I've brought two such brochures that we've used in period mailings to our customers to inform them of the need to take action. Our Enterprise Computing sales organization has conducted Y2K meetings with several thousand of larger customers around the world. Hewlett Packard has also informed our customers of any computing and health care products purchased directly from HP since 1995 which is not compliant, whether it's under a support agreement or not. Last, we provided our channel partners who resell HP products with Y2K information which they can provide to their customers.

In addition, these proactive communications programs HP's year 2K program offices around the world respond to customers' requests daily for information about the Y2K readiness of our products. These groups of HP employees answer questions, letters, faxes and surveys that customers may pose about Y2K. We've also made sure that all HP call centers and response centers worldwide and staff are trained to handle Y2K questions. HP's field organization is being equipped with the latest information on product compliance, services, upgrade programs for our customers and tools to assist customers with their Y2K readiness.

HP's central Y2K website has been active since early 1997 and is now attracting more than 250,000 visitors a month. Our website contains our product compliance data base listing status of the more than 100,000 current and past HP products Brad mentioned. For customers who do not have access to the Internet or our website, our call centers and sales and support offices will respond to any Y2K inquiry we receive.

We're working hard to inform the millions of customers who are not on a support contract with HP about our Y2K efforts. We're including a Y2K message in every press release the company issues in 1999, in the annual report, in select advertisements and direct mail campaigns in many countries and in key messages at trade shows and conventions such as at HP World next week in San Francisco.

The other manner in which Hewlett Packard will assist its customers' transition successfully to the next millennium is through our enhanced customer support capacity and providing additional self-help tools directly to our customers. HP expects that the year 2000 issue will increase the number of phone calls for support into our call centers and response centers. While we can't precisely predict exactly how many calls we will receive for year 2000 support, we anticipate an increase in customer demand as we reach the latter stages of 1999 and 2000, particularly around the New Year's period for the rollover weekend. We believe that we'll see the greatest increase between the period of November 1st, 1999 and March 3rd, 2000. To address the needs for additional customer assistance during this period, we've taken specific action as part of our enhanced support capacity program. We have increased the staffing at our support call centers over this past year. We have developed specific employee work policies governing employee vacations and availability not only over the rollover weekend, but also in the surrounding months as well, not only for our call center and engineering personnel, but also the labs that are the escalation paths for those organizations. We have plans to redirect other HP resources on customer assistance activity should that be the case, and we've implemented new support tools and technology to more easily provide assistance to our customers including enhanced self-help tools that are available on our year 2K website.

The year 2K rollover weekend and surrounding period is certainly not expected to be business as usual. Our customer support response centers will be open for the rollover weekend to provide Y2K assistance for our customers. In fact, for that weekend we will also expand our after-hours coverage staffing in our response centers to provide additional support. As another way additional information and assistance will be provided to our customers around the clock, HP will be implementing a fast track method to identify, analyze and report Y2K issues through our electronic support center website to customers worldwide later this year. This is an enhancement under an already existing feature that we have in our support response centers.

In conclusion, the year 2K rollover and the surrounding period will be a time HP will ask all employees to focus on assisting our customers. HP is committed to making the transition to the next century a successful one for our customers and for our company, and certainly Hewlett Packard thanks you for the opportunity to share our year 2000 program with you today.

[The information referred to follows:]

HEWLETT®
PACKARD

START HERE

THE FIRST STEP TO MAKE YOUR HP SYSTEMS YEAR 2000 COMPLIANT

START RIGHT

START NOW

The Year 2000 is approaching fast, and if you haven't tested your HP computer systems, you should. This guide is a good place to start. Read it for information about the Year 2000 operating system compliance of your HP computer systems. Then visit HP's Year 2000 web site for more detailed information about the Year 2000 status for all HP products.

TEST NOW

www.hp.com/year2000

This guide is designed to help you. The first step to make your HP systems Year 2000 compliant is to identify which hardware platform and operating system you have, then read the appropriate section. It is your responsibility to take action on the information.

HP-UX Servers

You must install Year 2000 patches for HP-UX 10.01, 10.10, 10.20, and 11.0 to be compliant. These patches are available through our web site www.software.hp.com/products/Y2K/coredepot.html.

We recognize that a customer's environment may include applications that stress the operating system differently. Therefore, it is possible some customers may identify issues that need to be resolved. If a new patch is created, it will be posted to the web site listed above. You can register on this web site to automatically receive any significant patch updates.

HP-UX 9.04 is obsolete, will not be made compliant, and must be upgraded. It reached the end of its extended support life at the end of 1998. To make the upgrade process easier, we've recently announced a comprehensive 9.04 upgrade program. The recommended version of the operating system for Year 2000 compliance is HP-UX 10.20 and 11.0. For more information, please visit www.hp.com/year2000.

For the latest compliance information for HP-UX application products on your system, please check HP's Product Compliance Status database periodically at: www.hp.com/y2kdb/index.html.

SPP-UX and Convex OS

SPP-UX 5.3 for the SPP2000 and SPP2200 are Year 2000 compliant with a patch that was available June 1, 1998. Similarly, compilers, tools, and libraries for these systems are also compliant with Year 2000 patches. All patches are available from HP's Richardson (Texas) Patch Center. Patches for SPP-UX 5.3 for the SPP1200 and SPP1600 became available December 1998. The SPP2000 and SPP2200 platforms (hardware and diagnostics) and the SPP1200 and SPP1600 platforms (hardware and diagnostics) are now Year 2000 compliant. Versions of SPP-UX before 5.3, all Convex OS versions, and the SPP1000 platform are not Year 2000 compliant and will not be made compliant.

HP-UX Workstations

All of HP's PA-RISC workstations have Year 2000 compliant hardware. The operating system situation is a bit more complex. HP-UX 10.20 and HP-UX 11.0 are Year 2000 compliant with patches. These Year 2000 patches must be installed to make these releases fully compliant. Please visit the HP Year 2000 web site at: www.hp.com/year2000, to find out how to get information on these patches. HP-UX 9.0X releases, 9.01, 9.03, 9.05, and 9.07, are now obsolete and beyond support life; these releases are not Year 2000 compliant and will not be made compliant. The recommended version of the operating system for Year 2000 compliance is 10.20 and 11.0.

The HP Motorola 68000–based Series 300 and Series 400 workstations are Year 2000 compliant, running the HP-UX 9.10 version of the operating system with Year 2000 patches. HP-UX 9.10 is the only supported version of the operating system. All Year 2000 patches are posted on the Electronic Support Center web page.

The HP Apollo/Domain operating system versions 10.3.5.15 and 10.4.1.2 are

Year 2000 compliant with patches. All Year 2000 patches are posted on the Electronic Support Center web page.

Even though HP-UX 10.20 and 11.0 are Year 2000 compliant with patches, applications that do not currently process Year 2000 date information correctly will continue to process it incorrectly and would do so even if your operating system were compliant. You need to test that your applications will handle date information properly.

MPE/iX

HP has released Year 2000 patches that, when installed, make MPE/iX Release 5.5 Express 4 Year 2000 compliant. If you have a previous version, you must upgrade to MPE/iX 5.5 Express 4 and install the Year 2000 patches to be compliant. MPE/iX 5.5 will be a supported version through the end of 2000. MPE/iX Release 5.5 Express 4 is available to customers with valid HP software support agreements at no additional charge.

HP Predictive Support and Diagnostics for HP-UX and MPE/iX

Systems that run HP Predictive Support need to be updated to an HP Predictive Support version that contains a Year 2000 patch by the end of 1999. These are the first versions of HP Predictive Support containing the Year 2000 patch:

HP-UX 10.01 - C.10.R1 (Will be released via patch PHSS_17493)

HP-UX 10.10 - C.10.1Y (Will be released via patch PHSS_17494)

HP-UX 10.20 - C.10.21 (Will be released via patch PHSS_17495)

HP-UX 11.0 - C.11.0m (Will be released via patch PHSS_17496)

For all HP-UX 10.X through 11.0 releases running Predictive, the Support Tool Manager diagnostic system is required for proper Year 2000 operation. Although Support Tool Manager was designed to be Year 2000 compliant, the certification testing was actually performed on version A.10.00 of Support Tool Manager. This version was first released in April 1998 with the Diagnostic Independent Product Release (IPR) 9804 Media.

Customers must update their systems to the Diagnostic IPR 9804 Media or later release for Support Tool Manager to be Year 2000 compliant.

MPE/iX 5.5 - B.55.08 (Will be released via patch OSPKXP0 [A])

MPE/iX 6.0 - B.60.02 (Will be released via patch OSPKXP1 [A])

The diagnostic software on these MPE/iX releases is Year 2000 compliant.

Any system with a support agreement and with a version of HP Predictive Support less than that shown above needs a newer version. If your system needs a newer version of HP Predictive Support, you can install the current patch from the Electronic Support Center web site at: http://us-support.external.hp.com.

HP NetServer Systems, HP Vectra Commercial PCs, HP Kayak PC Workstations, HP Brio Business PCs, HP OmniBook PCs, HP Pavilion PCs, and HP Palmtop PCs

Since every HP NetServer system has a built-in real-time clock chip, HP NetServer systems are generally Year 2000 compliant. The exceptions to this, where the system resets back to 1980, are:

HP NetServer LC (4/66, 4/100, and 5/66) systems

HP NetServer LE and LF systems

HP Vectra 486 S20, ST, T, and U NetServer systems

These systems will need to have the real-time clock reset on January 1, 2000, or have the BIOS upgraded.

All HP Vectra PCs, HP Brio PCs, and HP Kayak PC workstations introduced since the end of 1995 meet both the National Software Testing Laboratories (NSTL) YMARK2000 certification and HP's own rigorous compliance standard.

HP has made available a new version of the system BIOS for the Pentium® and Pentium Pro-based HP Vectra PCs, introduced prior to the end of 1995, that will manage the Year 2000 transition correctly. These new BIOS versions are available through the Tools section of the HP Year 2000 Desktop web site: www.hp.com/desktop/year2000.

The HP OmniBook 800 notebook PC, introduced in the fall of 1996, is Year 2000 compliant. For the HP OmniBook 5500 notebook PC, HP has developed a new version of the system BIOS (v 2.12) that will handle Year 2000.

All HP Pavilion PC hardware is National Software Testing Laboratories-certified as Year 2000 compliant and is expected to handle the rollover to the Year 2000 without any problems. In addition to passing a stringent set of corporate criteria, HP Pavilion PC hardware also complies with NSTL's testing requirements for Year 2000 compliance. Our PC hardware along with our BIOS (the software that helps the operating system communicate with the hardware) and our real-time clock, all support the HP Pavilion PC's ability to recognize four-digit dates necessary to successfully change to the Year 2000.

All HP Palmtop PCs are capable of handling the date roll to Year 2000 and beyond, unless a user-installed application bypasses the operating system and BIOS to retrieve the date directly from the real-time clock. You should work directly with your application suppliers to ensure that their products are Year 2000 compliant.

Many corporate networks are configured to synchronize all PC clients' internal clocks to the date and time kept on the server. These network-connected PCs would then have the date set to the correct value by the server automatically.

Although applications generally get the date and time from the operating system, some applications still only use two digits to store the year. Since there are so many applications, HP recommends that you check with your software suppliers about the required actions to ensure that your PC and HP NetServer applications will be Year 2000 compliant.

HP's operating-system suppliers for the above products have advised HP that they are addressing the Year 2000 issue. Several operating-system suppliers have already announced that their operating systems will detect a date that rolls incorrectly, and it would then prompt the user to change the date or correct it automatically. You also have the option of setting the correct date on January 1, 2000, by using the BIOS setup menu. You need to contact your operating-system supplier for the latest Year 2000 information on their products.

You Have the Right Start.
Test Your Systems Now.

HEWLETT® PACKARD

HP has made every effort to ensure the accuracy of our product testing. However, because your environment is different from HP's laboratory test environment, it is your responsibility to validate the Year 2000 readiness of these products in your own environment. Therefore, information about the Year 2000 status of HP products is provided "as is," without warranties of any kind, and is subject to change without notice. HP makes no representation or warranty respecting the accuracy or reliability of information about non-HP products. Such information, if any, was provided by the manufacturers of those products and you are urged to contact the manufacturer directly to verify Year 2000 readiness. The information provided here constitutes a Year 2000 Readiness Disclosure for purposes of the Year 2000 Information and Readiness Disclosure Act in the United States.

Printed in USA M0599
Americas
P/N 5968-5781EAM

HEWLETT® PACKARD

DON'T RISK IT

MAKE YOUR HP SYSTEMS YEAR 2000 COMPLIANT NOW

DON'T WAIT

TEST NOW

The Year 2000 date problem could wreak havoc with your information system if your hardware and software are not Year 2000 compliant. This guide contains critical information about the Year 2000 compliance status of your HP-UX operating system and lists numerous HP resources that can help you get ready.

UPGRADE NOW

www.hp.com/year2000

This guide contains information about the compliance of HP-UX operating system products. HP recognizes that not all of our HP-UX operating systems customers may have a current support agreement, or may be receiving support on a non-compliant version of the HP-UX operating system. This guide will lead you to resources that can help you check your products for compliance, order upgrades, and request patches. More information is readily available to you. Simply call HP Service and Support at 1-877-470-4715 or e-mail your inquiries to y2k_email@hp.com.

General Information About Upgrading the HP-UX Operating System

HP-UX 9.0X and earlier HP-UX versions are not Year 2000 compliant and will not be made compliant. Fully supported versions of HP-UX (10.0X or higher) are compliant only when all current Year 2000 patches are installed. Some HP software applications may also require that you upgrade to compliant versions and install all patches beyond those needed for the operating system.

Software applications that do not currently process Year 2000 date information correctly will continue to process it incorrectly and would do so even if your operating system were compliant. You will only know if you are ready for Year 2000 by testing your systems to ensure they process date data correctly.

Since your environment may include applications that place stress on the operating system, it is possible that some issues could be identified that need to be resolved. Test your environment now.

Upon installation of all Year 2000 patches, the following operating systems are Year 2000 compliant:

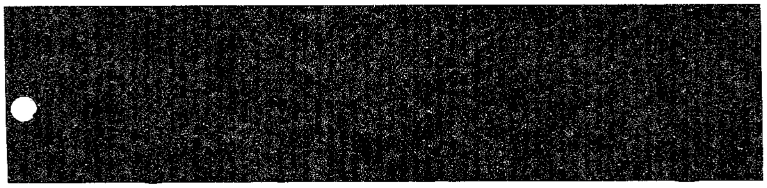
- HP-UX 10.0X or higher
- SPP-UX 5.3; Versions of SPP-UX before 5.3 and all ConvexOS versions are not Year 2000 compliant and will not be made compliant
- HP Motorola 68000-based workstations running the HP-UX 9.10 version of the operating system
- HP Apollo/Domain operating system versions 10.3.5.15 and 10.4.1.2

HP Predictive Support, available to support agreement customers, needs to be updated to a version that contains a Year 2000 patch. The Support Tool Manager diagnostic system, Diagnostic Independent Product Release 9804 media or later release, is also required for proper Year 2000 operation.

You will also need compliant versions of HP or non-HP application software. Please check with the manufacturer of your application software to obtain the Year 2000 compliance information. To check the Year 2000 compliance on other HP products, check the HP Year 2000 web site at www.hp.com/year2000.

HP has several programs available to assist with your migration to a Year 2000 compliant version of HP-UX operating system products. We encourage you to take advantage of these programs and to establish a migration plan as soon as possible. In addition, HP recommends testing your applications in your environment to determine your system's overall Year 2000 readiness.

There are support limitations for customers who continue to run Year 2000 non-compliant products.



Here's How HP Can Assist You

HP recommends that you install all Year 2000 patches.

Year 2000 Patches can be downloaded at www.hp.com/year2000/products/patch.html. Select 'Support for Servers and Workstations' to get to the Electronic Support Center (free registration); also, the y2koscheck Tool lists current Year 2000 patches. If new Year 2000 patches are created, they will be posted to this web site.

HP-UX 9.04 Upgrade Program for Servers provides free operating system software and selected languages and middleware upgrades from HP-UX 9.04 (or earlier) to Year 2000 compliant HP-UX 10.20. Visit www.hp.com/go/9000customer. For systems on support, this upgrade is available as part of your support agreement.

HP-UX 10.20 Year 2000 Transition Kit for Workstations provides a compliant operating bundle for all HP-UX 9.0X customers, free. Order P/N B6815AA with appropriate language option. Visit www.hp.com/unixwork/y2k/y2k_menu/y2k_upgr/oskit.html for more details and visit www.hp.com/go/visualize under 'OK with Y2K' for additional information on HP-UX workstation Year 2000 programs.

HP-UX 9.10 for Motorola 68000-Based Workstations provides the HP-UX 9.10 upgrade base product, media, and any additional licenses for a charge. Visit www.hp.com/go/vintagesw.

HP-UX 9.0X Guidance and Technical Assistance is available, free. Visit www.hp.com/year2000/hpux_90x_techasst/need/upgrade_prog.html.

Domain/OS Year 2000 Patch Bundle offers Year 2000–compliant DOMAIN/OS 10.3.5.15 or DOMAIN/OS 10.4.1.2 for a charge (Year 2000 patches must be installed). Visit www.hp.com/go/vintagesw.

HP Predictive Support, with Year 2000 patches, is available for support agreement customers—if your system needs a newer version of HP Predictive Support, you can install the current patch from the Electronic Support Center web site http://us-support.external.hp.com.

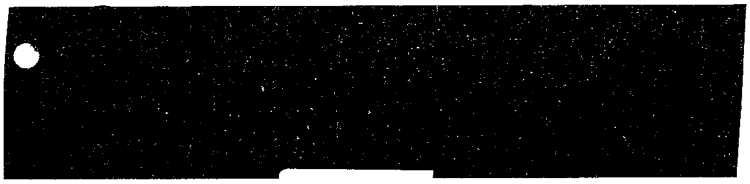
The HP Product Compliance Status Database is available at www.hp.com/y2kdb/index.html.

TradeUp '99 for Servers allows you to trade in your HP 9000 Enterprise Servers and receive a rebate toward the purchase of a new server. Rebates are available on select HP 9000 Server models. Visit www.hp.com/year2000/help/upprograms.html.

Power Up with HP, HP-UX Workstation Hardware Replacement Program allows you to upgrade the hardware on a HP-UX 9.0X or Domain/OS-based system and receive rebates on a new HP-UX workstation. For details, visit www.hp.com/go/poweruphp.

HP Welcome Back '99 Program is a special service promotion that waives some of the return-to-support fees with the purchase of certain HP support services. Call HP support at 1-877-470-4715.

Operating System Update Planning and Implementation
If you are interested in upgrade assistance to HP-UX 10.20, call HP support at 1-877-470-4715 for details.



HP-UX System Administration Services include:

- Operating system migration planning
- Software patch management
- System administration services for HP-UX, MPE/iX, NT, and Novell
- Performance services (that is, HP OpenView and Oracle products)
- MC/ServiceGuard services

For details, call HP support at 1-877-470-4715.

HP Year 2000 Assessment Service will help determine the Year 2000 compliance status of your HP products and, where applicable, indicate recommendations to achieve product compliance. For details, call HP support at 1-877-470-4715.

HP-UX Transition Courses offer the following five courses:

- New features and functions of HP-UX release 10.X (video)
- Additional new features and functions of HP-UX 10.X (video)
- Hands on with HP-UX 10.X: Upgrade Tools, System Administration Enhancements, and Software Distributor (video)
- New features and functions of HP-UX 11.0 (seminar)
- Hands on with HP-UX 11.0 (workshop)

For details, call HP support at 1-877-470-4715.

Year 2000 Planning and Methodology Course is a three-day course on the planning and implementation of Year 2000 procedures based on Data Dimensions Ardes 2K™, an innovative and automated technology transfer process. For details, call HP support at 1-877-470-4715.

Year 2000 Support Limitations

Customers who continue to run HP-UX 9.0X or an earlier version are at risk because the software is not Year 2000 compliant and is subject to support limitations. You must be on the current version or immediately preceding version of HP software to receive full contractual support. Some customers may not be in a position to migrate to a supported HP-UX version today. For existing support customers who need additional time to implement their migration plan, HP will provide contractual support for HP-UX 9.0X or earlier for a limited time, using commercially reasonable efforts as determined by HP. Support will be limited to patches or workarounds for known defects. HP will not provide new product features/enhancements, new peripheral support, nor documentation updates. HP will not create new patches or new workarounds for any problems, including those related to Year 2000 non-compliance. No additional fixes will be provided if one does not already exist.

Customers running HP-UX 9.0X or earlier on their systems remain solely responsible for upgrading to a Year 2000 compliant product. HP will not be liable for any failures arising from the Year 2000 non-compliant status of HP-UX 9.0X or earlier, or from your efforts to make HP-UX 9.0X Year 2000 compliant.

HEWLETT®
PACKARD

HP has made every effort to ensure the accuracy of our product testing. However, because each customer's environment is different from HP's laboratory test environment, it is your responsibility to validate the Year 2000 readiness of HP products in your own environment. Therefore, information about the Year 2000 status of HP products and Year 2000 services are provided "as is" without warranties of any kind and is subject to change without notice. HP makes no representation or warranty respecting the accuracy or reliability of information about non-HP products. Such information, if any, was provided by the manufacturers of those products, and you are urged to contact the manufacturer directly to verify Year 2000 readiness. The information provided here constitutes a Year 2000 Readiness Disclosure for purposes of the Year 2000 Information and Readiness Disclosure Act in the United States.

Printed in USA M05/99 P/N 5968-5780EAM
Americas

Mr. HORN. Well, thank both of you very much. If I had my checkbook here, I'd sign up right now. You two are real marketers.

So I'm looking forward, Mr. Hall, to your marketing also. You're with one of the great firms of this valley, and that's the Intel Corp. Richard Hall is the director of California governmental affairs and the year 2000 program manager.

Mr. RICHARD HALL. Thank you, Mr. Chairman. Actually, as I listened to Hewlett Packard's testimony, I could probably say ditto to about 99 percent of it, because our programs are very much in parallel with theirs as a similarly structured company in the same industry. But let me stick to my planned remarks with a few extra comments.

First, I want to express our thanks as an industry and company to this subcommittee. I believe that in unison with Chairman Bennett's committee in the other house, that you have achieved a very high level of public attention for the year 2000 problem that otherwise would not have been achieved. In particular, the report card methodology that you've used on a quarterly basis has focused media and public attention to that, and to me it's really a case study in how to succeed in getting attention to something that's very difficult to get attention to on a good day.

Mr. HORN. Well, thank you. It does have its impact. The State Department finally cleared up their small number of mission-critical systems, and somebody asked them from a computer journal, "How did you finally do it, the move from the F to the A-minus stage?" And they said, "Well, I guess my boss was just tired of all those Fs." So it helped.

Mr. RICHARD HALL. Precisely. In that context, it's not in my prepared testimony, but in listening to the public sector representatives this morning, I wanted to make this remark. For another presentation I did on the year 2000 recently on July 30th in a nice place up in South Lake Tahoe, I did an analysis of 1 day's news media coverage regarding the year 2000. I picked an interesting day. It was July 21st, 9 days before I was up there, and on that day there was a good news development on the year 2000 and a bad news development.

The first was Mrs. Garvey's announcement that the FAA had achieved, and she said without qualification, full compliance on the year 2000, and the public should have no concerns. On that same day, Mrs. Williams-Bridgers of the U.S. Department of State testified before the Congress that one-half of the 161 countries that the U.S. Department of State had analyzed around the world for year 2000 capability had the potential for severe infrastructure disruptions which would in turn effect U.S. trade and commerce in significant ways.

Now, the following day, July 22nd, in the 30 major U.S. daily newspapers there were seven stories about Mrs. Garvey's announcement and about Ms. Bridger's testimony. There were 130 stories about day six of the Kennedy/Bessette tragedy, a 16 to 1 ratio. I'm not drawing a value judgment there, but I'm pointing out where attention has been focused in the American public mind and conscience about this, and a concern that I would express is that as we get closer, today we have 139 days remaining until the date rollover, as we get closer, the public and media attention will shift from very low gear to extremely high gear. We'll go from an under reaction to an overreaction, and this parallels comments made by some of the representatives today of the municipalities who are struggling to develop and execute public information campaigns.

Now after my editorial diversion, I will return to my text and a few comments, and I'll tell you about Intel. The other task that this subcommittee and Chairman Bennett's committee on the Senate side played such an important role in achieving was the final passage of H.R. 775, known as the Y2K Act, signed by the President on July 20th. I took note at the time that that bill was signed by the President Pro Tem of the Senate, Senator Thurmond, who will turn 97 years old on December 5th, still the oldest American political leader, electronically signed the bill and transmitted it by e-mail to the White House for the President's signature. I thought that was an historic development in and of itself. It creates a necessary legal framework for potential litigation over the year 2000 and over the next 3 years, and was a milestone development for this country.

Let me offer you in my brief time four observations from Intel Corp.'s standpoint. First of all, 10 days ago we announced internally, and I'm delighted to announce the same externally today, that Intel Corp. had achieved 100 percent, and again, 100 percent, not 99.9 percent, compliance of all internal systems. Of all the applications and systems that run Intel's business systems worldwide, we are now complete.

No. 2, as of today, by our own internal measurement methodology, 95 percent of our mission-critical and priority suppliers around the world are either year 2000 capable or have contingency plans in place that have satisfied us in terms of the capability of continued support of Intel's business.

Third, on a less bright note, we continue to have concerns at Intel about the readiness of external infrastructure, power, telecommunications, water, transportation in certain critical foreign geographies. Our experience, my own experience as part of Intel's year 2000 team traveling to a number of foreign countries, I spent nearly 2 weeks in Japan in May as one example, parallels what the State Department has found. In fact, I coincidentally crossed paths twice with the State Department team in the month of May. We were on some of the same airplanes and going to some of the same places, meeting some of the same people. That experience also parallels what the GartnerGroup has publicly described for the U.S. Congress and the media about the concerns regarding foreign infrastructure and its readiness, particularly in Asia and the Pacific.

Last, in brief summary I'd like to say, as Hewlett Packard remarked, our public website which is www.intel.com contains a vast wealth of information about our year 2000 readiness, our products, our strategies, our programs, far more than I could adequately summarize today. Under the guidance of Congress established in October 1998 under the first major Federal law that was passed, we have done as full a job of disclosure as I think we are able to do about all aspects of Intel's year 2000 readiness.

So again, I'd like to thank you, Mr. Chairman, and your subcommittee for an excellent job of oversight and drawing public attention. We'd like to thank you for the legislation passed in July, and I hope that I've given you an adequate overview of Intel's position today at 139 days before the date rollover.

Mr. HORN. Well, that's a very helpful statement, and we'll get into some of the foreign experiences in the question period here. They're very important.

[The prepared statement of Mr. Richard Hall follows:]

TESTIMONY OF
RICHARD C. HALL
MANAGER-CORPORATE GOVERNMENT AFFAIRS
INTEL CORPORATION

BEFORE THE U.S. HOUSE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION AND TECHNOLOGY, COMMITTEE ON GOVERNMENT REFORM

AUGUST 14, 1999
SAN JOSE, CALIFORNIA

THE YEAR 2000 CHALLENGE AT 139 DAYS TO GO

Mr. Chairman, members of the Subcommittee, thank you for inviting me to be here today to offer Intel's and the U.S. semiconductor industry's current perspective on the Year 2000 challenge.

Let me also express my industry's thanks for this subcommittee's extremely valuable oversight actions since June 1998. You have brought a sharp focus of resources and news media attention to necessary remediation of the U.S. government's mission-critical functions.

By my count, this subcommittee has held 20 hearings about the Year 2000 problem in the past 14 months, including 11 previous field hearings like this venue today. Your "report card" methodology for grading U.S. government Year 2000 readiness has been a case study of success in how to focus news media attention on a critically important subject. This subcommittee's work also laid the groundwork for the passage and signature by President Clinton July 20 of H.R. 775, the Year 2000 Readiness and Responsibility Act, which creates a necessary new legal framework for managing potential litigation resulting from Year 2000 problems.

In my limited time today, let me offer you four points to you about Intel Corporation's status with respect to solving the Year 2000 problem:

1). Ten days ago, Intel Corporation announced internally that 100 per cent of our critical and priority applications are year 2000 capable. These are the internal applications and systems that run Intel's worldwide business.

2). Ninety-five per cent of Intel's mission critical and priority suppliers are either Year 2000 capable or have contingency plans in place to minimize risk, based on our internal certification methodology.

3). External infrastructure readiness (power, telecommunications, water, transportation) remains a key concern in some non-U.S. geographies. Intel is focusing its efforts on driving these remaining offshore problem areas to resolution in the next 139 days.

4). Intel's public web site, www.intel.com, contains a direct link to all of Intel's public information regarding company strategy, product readiness, PC remediation advice and other related Year 2000 topics. This site and its links contain far more than I can summarize for you today. It is our central public information resource, fulfilling the obligation we have defined for ourselves and the Congress has defined for U.S. businesses under the Year 2000 Information Readiness and Disclosure Act signed into law in October 1998.

A Semiconductor Industry Overview of the Year 2000 Problem

Semiconductors have become a part of everyday life; they exist in everything from coffee makers and alarm clocks to advanced computers and electronic equipment. In part due to the pervasiveness of the semiconductor industry's products, there is a misperception being perpetuated that the Year 2000 problem is somehow a "chip problem." I would like to address and clarify this misperception.

From Intel's perspective, it is important to point out that our long-time flagship product, microprocessors that run personal computers, do not contain (and never have contained) any date-dependent functions. The software running on the microprocessor may have date-dependent functions, but not the microprocessor hardware itself.

As you know, the Year 2000 challenge stems from a decades-old practice of sorting and processing dates in a two-digit format, a practice that emerged when conserving computer memory was considered essential because of its high cost. What this means from a practical viewpoint is that electronic products that process dates in this way, which could include everything from computers to the family VCR, may not know whether "00" means the year 1900 or the year 2000. Another date-related issue that companies are confronting arises from the practice of some computer programmers who use "dummy dates" such as "99" and "00," which can trigger system shutdowns and other effects when dates that include those numbers are reached. Because electronic products are highly integrated into today's world, these problems can have far-reaching effects.

Evaluating whether a product is Year 2000 ready is quite complicated. Many electronic products are collections of semiconductors and other parts that operate and interact according to instructions supplied by software. It is the interaction of all these hardware and software elements that determines whether a particular product is Year 2000 ready. To complicate matters, many elements found in the same product may have been made and/or programmed by different companies.

The Unique Challenges Facing the Semiconductor Industry

The semiconductor industry faces a considerable challenge in evaluating Year 2000 readiness issues. There are thousands of different kinds of semiconductors. The vast majority of semiconductors are incapable of generating, comparing or sorting date information. These semiconductors are unaffected by the Year 2000 issue. A small percentage of semiconductors are capable of generating or processing date information when software is added to the chip: the software is typically specified and owned by the customer, not the chip maker. An even smaller number of chips have circuitry that is designed to generate or process dates, and even in this category the chipmaker may be manufacturing to customer specifications.

In general, chip makers do not design or develop the programming for their products: In fact, typically the programming is the proprietary material of the third party that developed it, not the semiconductor manufacturer. Even when the chip maker has access to the programming — which is provided as a series of zeros and ones — it typically is not permitted by confidentiality agreements to verify through reverse-engineering that the product is Year 2000 ready. For similar reasons, if a semiconductor manufacturer has been asked to manufacture to a design supplied by a customer, the chipmaker can't determine whether the semiconductor is Year 2000 ready.

Further complicating this issue is the fact that semiconductors are an integral part of larger "embedded" systems that affect the operation of a myriad of electronic products. Embedded systems provide control functions in numerous products, from the family VCR to microwave ovens to cars. Embedded systems have the ability to compute. Typically, these systems also contain instructions — usually in the form of software — that determine how the end product operates and what it computes. Again, these instructions are usually not developed by the chipmaker, but rather by the manufacturer of the end product.

Another critical issue is how the semiconductor device will work as part of an electronic product, which may contain other parts that are not Year 2000 ready. For example, a typical electronic product such as the family computer contains a collection of parts that work together. It is the interaction of all these elements that dictates whether the product is Year 2000 ready. In the case of the computer, these parts include the microprocessor, the BIOS (Basic Input Output System) that controls the interface between the operating system and the computer hardware and controls the system's real-time clock, the operating system and the software applications. Because the readiness is determined by the interaction of all its various components, the manufacturer — or in some cases the distributor or owner — of the finished electronic product is the only entity capable of testing and evaluating whether the product is Year 2000 ready.

I hope this statement helps explain the relationship of "embedded systems" and chips to the Year 2000 issue. As I have already noted, the ultimate solution to this question is beyond the control of the semiconductor supplier. Chipmakers can and will continue to assist their customers by providing information. Ultimately, the manufacturer of the finished electronic product is the only one capable of determining how the elements of the system function together as an integral unit and whether the product is Year 2000 ready. And at the consumer level, individuals and businesses must contact the manufacturers of electronic products to determine whether they are Year 2000 ready.

Mr. HORN. Next we have a 2-day involvement with this subcommittee. Tom Latino is the product manager for Pacific Bell. He was with us in our Sacramento hearing yesterday, and we're delighted to see you again.

Mr. LATINO. Good morning. My name's Tom Latino and I am the director of the public safety organization for Pacific Bell. I appreciate the opportunity to update to you on SPC's readiness for the year 2000, and I'm happy to say we have some great news to share.

The bottom line is that when you pick up the phone on January 1st, our network will be ready to serve you just as it always has, and so will the wireless, data, Internet and other services we provide. We spent nearly 4 years preparing for the Y2K issue. As of June 30th, virtually all necessary Y2K upgrades have been completed. A very few upgrades are scheduled to be completed by September.

As we wrap up these upgrades, we will continue to focus on testing and finalizing our business continuity plans. All of our services will be tested and retested in simulated year 2000 environments prior to January. Our testing efforts also go well beyond our own network as SPC is working with the Alliance for Telecommunications Industry Solutions, or ATIS, to test our services in conjunction with other communication companies and other industries. As a matter of fact, ATIS recently announced the successful completion of recent Y2K tests involving communication networks serving the credit card and financial industries. SPC and other communication carriers had no difficulty in transmitting financial data in the simulated environment.

We have also worked closely for Telephone Year 2000 Forum which in December completed tests showing that local networks are prepared to provide uninterrupted service. This internal and third-party testing provides further evidence that Y2K will be a non-event for our customers, and while we strongly believe that will be the case, we also recognize that factors outside of our control could potentially impact our service. To further ensure continuous quality service, SPC is enhancing its business continuity plan to prepare for Y2K contingencies. The plans are an extension of Southwestern Bell's existing procedures for providing service in the event of an emergency or natural disaster.

As part of these business continuity plans, SPC will increase staffing and customer support at business centers during peak periods leading up to and including the New Year's holiday. We are also establishing command centers throughout our service territory to ensure a smooth transition to the New Year.

As you can tell, Y2K readiness has been a very big job. All told, SPC has spent nearly $200 million to prepare for Y2K. SPC's Y2K project management team is led by an officer of the company and each of our major business units have a dedicated Y2K coordinator responsible for managing our year 2000 issues within their organizations. To keep our customers up to date on our progress, SPC's Y2K team maintains a comprehensive website with the latest information available. Anyone looking for detailed information on our Y2K readiness can access the preparing for the millennium section on SPC's website at www.spc.com. This site includes a section that allows you to check on the readiness of the central office switch that serves your community. You can also register at the website to receive a copy of SPC's final readiness report.

Thank you again for the opportunity to provide this update.

Mr. HORN. Well, thanks very much, and we do want to list all your numbers so people can reach you. That's a very good service you all have on that.

Mr. Ralph Tonseth is director of aviation for San Jose International Airport. I must say I always enjoy coming in and out of San Jose. You run a very good operation there. Where does that rank in the airports in California, just as a curiosity?

Mr. TONSETH. Mr. Chairman, San Jose International Airport is currently the fourth largest airport in the State of California, currently handling more than 11 million passengers annually and 250 million pounds of air freight annually. At the current time, we also are the employment site for more than 5,300 individuals and are the only commercial airport in the Santa Clara County, and therefore the Silicon Valley for the provision of commercial air services, and so we therefore take the responsibility very seriously to support all of these great corporations and the transportation needs both for individuals' trips and for air cargo services.

I'd like to thank you, Mr. Chairman, for the opportunity to present to this subcommittee the report of San Jose International Airport on our Y2K program. Like many others, we have long recognized the need to address what has been called the millennium bug problem, and we began our program in the summer of 1997, and since that time have expended internally more than 10,000 staff hours and expended more than $6 million to reduce the chance of service interruptions related to potential Y2K problems. I'd like to give you just a very brief overview of our program, since it really does integrate many sectors of our local economy.

Under specific direction from the FAA, we have identified all mission-critical systems related to air transportation, both in hardware, software and embedded chips that may impact airport operations for the year 2000. We've also been working on an ongoing basis with suppliers both from the private and public sectors to ensure us that their systems that we use are compliant and therefore will not negatively impact passenger or freight customers.

Early on we performed a set of risk analyses and set priorities for compliance, and we have, to the best of our ability, confirmed by means of testing that all airport critical systems and equipment do meet the year 2000 requirements. We expect to have all of our airport systems, with the exception of our parking and revenue control systems ready by September 30th, 1999. That system, the Parking Control System will be Y2K compliant by November. We've developed detailed contingency plans for all systems, and those plans have been antiquated with our existing emergency operations programs.

The scope of our program at the airport has been extensive. We have identified 54 critical systems containing over 4,000 individual components. Each of these systems has been thoroughly reviewed and assessed to determine the level of risk, and in addition, each of these system's potential for health, safety and other impacts have been evaluated.

We also have invested in hiring two independent consultants and have gained from them considerable insight into the year 2000 program. The first of these was a consultant that provided an embedded chip inventory, which we completed in May 1998. And the second firm provided us a project management and documentation expert.

The current status as of today is that eight critical airport systems that were found to be deficient have been replaced totally or upgraded and tested. 26 systems were found not to have embedded time/date components within them. These, however, have been also tested and replaced or upgraded where feasible. Five systems are currently being replaced as we speak and are expected, as I mentioned earlier, to be completed by September 30th. And we are currently working with other city departments, tenants or others and FAA to complete the compliance process for the remaining 15 systems we've identified.

We have made good progress, I believe, in dealing with this problem. We have allocated the appropriate time in staff and resources to deal with it. Our main concern as of today, really, is our dependence upon public utilities, fuel suppliers, telecommunication suppliers and others whose services are beyond our control. However, we will continue to work with these people to coordinate our efforts to make sure that we have everything up to date by the year 2000.

We will have on staff on the evening of December 31st, 40 additional personnel that would not normally be on station. We will open our emergency response center to deal with any potential problems that may arise, and as you may know from the new requirements from the FAA, we will, between midnight and the time we open for first operation the next morning, test, verify and report to the FAA at headquarters verification that all of our systems are working.

In conclusion, I'd like to thank the committee for coming to our nice city and holding this hearing, and I'd like to assure you that San Jose International Airport is up to date and really do aspire to make sure that if you do choose to land here on the morning of January 1st in your aircraft, I will be happy to meet you at the gate.

Mr. HORN. Thank you. We might do that. I was born in Santa Clara County, so I'm pretty familiar with this county.

[The prepared statement of Mr. Tonseth follows:]

SAN JOSE
INTERNATIONAL
AIRPORT

Subcommittee on Government Management, Information and Technology

Congress of the United States
House of Representatives

"Is Silicon Valley Prepared for Y2K?"
Hearing on Year 2000 Readiness
Saturday, August 14, 1999
San Jose City Hall

Statement of Ralph G. Tonseth, A.A.E.
Director of Aviation
San Jose International Airport

Good Morning, and thank you for the opportunity to present to this subcommittee, our report on San Jose International Airport's program for addressing the Year 2000 problem.

The San Jose International Airport has long recognized the need to address what has been called the "Millennium Bug" problem. The Airport began its Y2K Project in the summer of 1997, and since that time has devoted more than 10,000 staff hours and expended in excess of $6 million to reduce the chance of service interruptions related to a Year 2000 computer problem.

Overview of Program

The Airport, under specific direction from the Federal Aviation Administration (FAA), has identified software, hardware and embedded chips that may be vulnerable to Year 2000 problems to determine compliance of systems critical to Airport operations.

Staff has been working on an ongoing basis with our business partners (from both the private and public sectors) and suppliers to ensure compliance of systems that could negatively impact Airport passengers and customers.

Early on, the Airport performed risk analyses and set priorities for Airport system compliance. Since then we have been in the process of repairing, replacing and testing equipment and systems throughout the Airport.

Airport staff has confirmed by means of testing, that all Airport critical systems and equipment meet the criteria established for Year 2000 readiness. The Airport expects to have all Airport business systems and equipment with the noted exception of our Parking and Revenue Control System Year 2000 ready by September 30, 1999. The Parking and Revenue Control System will be Year 2000 compliant by November 1999.

Staff has developed detailed contingency plans for all Airport critical systems. These contingency plans are based on the Airport's existing Emergency Operations Plan, and they detail the procedures necessary to mitigate any service impact related to Year 2000 failures, either locally, or in the event of power-grid outages or utility system malfunctions. The Airport has also developed a Year 2000 Verification, Assessment and Recovery Plan for all Airport services. This document will serve as a detailed checklist for Airport staff for the period from December 30, 1999 through January 7, 2000. Staffing levels have been increased during the 1999-2000 holiday period as a precaution.

"Is Silicon Valley Prepared for Y2K?"
Hearing on Year 2000 Readiness
Saturday, August 14, 1999

Statement of Ralph G. Tonseth, A.A.E., Director of Aviation San Jose International Airport

Current Status (cont.)

During the next four and a half months, the Airport will continue to work toward Year 2000 readiness. Efforts will focus on:

- Continued Contingency Planning activities related to training and preparedness, including coordination of activities with other City departments as well as with Airport tenants.
- Continued reporting to interested parties Airport Year 2000 status information through presentations, interviews, surveys, etc.
- Continued monitoring of all purchases to ensure Year 2000 compliance as well as interface compliance.
- And we will continue to work with a variety of other City departments on Year 2000 compliance remediation, documentation and contingency plans for City systems that impact Airport services, such as communications, vehicles, equipment and fuel, financial systems and utility interfaces.

Conclusion

The San Jose International Airport has made good progress on work associated with Year 2000 compliance. Time and resources have been identified and committed to ensure that problems are corrected. Of concern is our dependence upon public utilities, fuel suppliers, telecommunication suppliers and other services beyond our control. San Jose International Airport will continue to work with these suppliers to coordinate efforts to ensure that we meet all Year 2000 challenges.

We have included in our contingency plans, processes, procedures, staffing as well as other resources to be available for a host of issues that might arise and we will continue our efforts to ensure that Airport services function normally on January 1, 2000 and beyond.

In conclusion, I'd like to thank the Committee for its time and attention to this issue and the opportunity to comment on the Year 2000 efforts made by the San Jose International Airport. If you have any questions, I would be happy to address them.

Mr. HORN. Now, let's go back, and if we can get Mr. Willemssen at the table, I think, my friend, that there's a chair right there. And I'd like to ask Mr. Willemssen, Joel, what have you heard from this panel that you'd like to bring to the floor, and we can talk about it.

Mr. WILLEMSSEN. I thought of a couple things that might be interesting, especially with HP and Intel here, is if they can give us a general perspective on what they think about embedded chips and the Y2K issue. Because if you look back at Y2K and how it's rolled out over the last several years, in the early years, this was really viewed as a mainframe issue, COBOL, and then after that, the embedded chip issue got a lot of play, a lot of concern. I think that's leveled off to some degree.

So to the extent that one can generalize on the embedded chip issue and on the extent of the IRTC problem, I think that would be useful.

Mr. HORN. How about that, gentlemen?

Mr. WHITWORTH. With embedded chips at Hewlett Packard, most of what we're looking at is as a user of these, whether it's a manufacturing production environment, or things that you read about, the elevators and escalators in office buildings and those sorts of things. In our testing, both in the facilities side of things and the manufacturing groups, as they've gone through testing, embedded chips have really not proven to be a significant issue at all. In very rare instances we found some things, usually in working with the manufacturer of that particular piece of equipment, we found that it's much lower expectation, or actual results than what we had expected to find. So it's been almost a non-issue for HP in terms of the embedded chip problem.

Mr. HORN. How about it, Mr. Hall? What's the Intel view on this?

Mr. RICHARD HALL. Two points: One is it's ironic in that about somewhere around 90, 99 percent of all of the chips or microprocessors that Intel has ever manufactured are the kind that go inside personal computers or servers, and by their very nature, they never have, now nor ever could have, any date dependent functionality. The software that runs on them may very well, but the hardware itself does not.

Over the years as really more of a sideline, we have manufactured as a company embedded process control chips, and I would concur with HP's general view both in terms of our internal operations and in terms of those products which over the years Intel has sold for embedded process control, that the problem turned out to be defined down to a much smaller scope than what was originally feared. A much smaller percentage of embedded process controllers actually have date sensitive functions, and most of those in turn have proven easier to remediate than originally thought.

However, there's a simple human fact here. It relates back to the observation, Mr. Chairman, that you made, which is one that we agree with. Year 2000 is a management and resource problem more than it is a technical problem, and even though the embedded process control issue in the United States with Intel or Hewlett Packard or worldwide is smaller than originally conceived as we've talked about, the fact is that if you don't go in and fix the thing, it will not operate correctly, and those organizations in any country's public or private sector that don't go in and fix and test directly are going to have significant failures, and that's an issue of management attention and resources. Those would be some observations I have.

Mr. HORN. How many embedded chips does Intel put out in year?

Mr. RICHARD HALL. I don't have that number today, Mr. Chairman. It's a relatively small number. If you look in terms of microprocessors we're probably manufacturing and selling somewhere around 10 million a month. Embedded process control would be a tiny fraction of that today. Very small. In the few 100,000, perhaps, if that.

Mr. HORN. Would it be fair to say that half of your sale of those would be to foreign countries and industry in foreign countries?

Mr. RICHARD HALL. About 55 or 60 percent of the corporation's sales today as a whole are outside of North America. So if the pattern parallels, for embedded process control parallels that, yes, sir, that would be correct, but I do not have full data for you today.

Mr. HORN. Could you just run through off the top of your head what the average citizen might run, think about, in terms of embedded chips in things that are very close to them in their house or in driving to work or in traffic signals, this kind of thing?

Mr. RICHARD HALL. All of those that you just mentioned, plus inside their VCR, their cellular telephone and several of the appliances they have around their home. All of us over the last few years have added more and more embedded process control in our lives. By some estimates, the average American has somewhere between 50 and 100 embedded process control devices surrounding him or her, and they have not ever seen a single one or actually know what they do.

Again, the good news is the vast majority, for instance, those in vehicles, primarily to the extent that they have a measurement of time, they measure things like the cycles that the engine turns over, not time according to the Gregorian calendar established by Pope Gregory IV in 1563, which is what actually got us into this problem. If you want to trace it back historically. I have a humorous story about that, I won't burden you with today.

Mr. HORN. Why not?

Mr. RICHARD HALL. Well, I've said in a few other venues that if you wanted to bring the ultimate witness before a public body, particularly the U.S. Congress, it would have to be Julius Caesar, because he established the Julian calendar in the first century. That calendar was with 12 months and X number of days and weeks and all that which we take for granted.

That calendar was then modified by Pope Gregory IV in the year 1563, and over the next four centuries, as Western Europe became economically and militarily and politically dominant, there is a period of European colonization, the rest of the world adopted the Gregorian calendar which originated in 1563.

Then in the second half of the 20th century, we taught the Gregorian calendar to our machines, and that's the historical lead-up to why we have this problem. If we developed a different calendar using some different counting system tracing back to Julius Caesar we wouldn't have had this hearing today. That's the historical reason for the year 2000 problem.

To try to answer your specific question, to complete my answer to your specific question, Mr. Chairman, in summary, the number of embedded process control chips that everyone relies on today is very large, but the vast majority of them, in fact, do not have date sensitive functionality that is going to cause them to fail at the millennium rollover. I hope that's a good summary answer.

Mr. HORN. It's very helpful. In some of our hearings we've been curious in terms of reactors, let's say nuclear reactors, other types of equipment that might be related to a power supply of one sort or another, and could something happen in terms of the distribution system once that energy is generated. Because obviously, we'll get more into it in the next panel, it's one of toughest problems we face is will your suppliers, let's say, have sufficient power to keep their lines going, and if they don't, we ought to know about it, because that really would be a problem.

So I don't know if any of you have any reaction to that.

Mr. LATINO. Certainly from SPC's perspective we have extensive power generation capabilities. We have reviewed all of our contracts with fuel suppliers to ensure that we will have a steady stream of fuel, and if you may remember, Mr. Chairman, approximately a little over a year ago a major municipality suffered or endured a power failure; the phone systems kept on working.

Mr. HORN. That's good news. Good ol' Ma Bell still lives.

Well, any other comments on Mr. Willemssen's point down there? How about it? You satisfied?

Mr. WILLEMSSEN. If I could, Mr. Chairman, indulge you in one related issue, yesterday you heard from two witnesses from two major health care providers that they have elected to test on their own their biomedical equipment rather than rely on what the manufacturers say. Most manufacturers of biomedical equipment say not to do that for fear of disrupting the device or getting false readings. HP mentioned early on in their statement that among their products are patient monitoring systems and other biomedical equipment items.

I was curious about what Hewlett Packard's view might be on major health care providers going out and testing biomedical equipment items on their own and what kind of impact it could have.

Mr. WHITWORTH. We actually have been encouraging all of our customers, whether it is a health care provider or a major corporation or nonprofit organization to do the tests.

But I think what happens in the industry is the HP equipment is used in an environment where it might be attached to another computer system, and you need to check those relays, the interface between the two. So while we can test our products in our labs, and we can come up with a company-wide testing process that we use for everything from our personal computers to our health care products, we then encourage people to take those products and test them in their own environment. So we are probably just the opposite of what you have heard, which is please do test and make sure that in your own environment, which is probably different from our own test labs, the thing behaves the same way that it does for us, and if it doesn't, tell us. We want to see if there is some sort of a problem that we haven't been able to discover, and fortunately that has not been the case in the health care side of things for HP.

Mr. HORN. When we were in Cleveland last year, we had a witness from the Cleveland Clinic, which is a rather well-known hospital complex in America, that they were checking all of their equipment, obviously, in the emergency room, and that there was a website where hospitals around the country could put on, A, the manufacturer's name, the model number, all the rest, and they wouldn't have to reinvent the wheel every day around the Nation.

Are you familiar with that, and are there other websites or other corporate websites you have where they can check your equipment and note what model they have and should they be concerned?

Mr. WHITWORTH. One of the beautiful things about the web, I think, it's allowed that degree of specialization to exist within industry groups and special user groups. We cooperate fully, provide them with the information that we have, and I think the sharing within the industry is also very, very important.

As I mentioned, a Hewlett Packard PC might have an Intel chip. It might be running a Microsoft piece of software and application, and we have established consortia where we will try to make sure the technical response is coordinated so that we don't end up pointing fingers at one another, and we come up with the adequate response that a customer might want. So somebody calls in to Microsoft and they determine it's HP, they know exactly where to go in HP to get the response, and the flip of that is true as well.

Mr. HORN. How about Intel on that? Is there a way your customers can get back in in relation to the chip problem?

Mr. RICHARD HALL. Yes. We have a large number of people, in fact, coincidentally most of them reside where my office is located near Sacramento in a town called Folsom. Several hundred people in our customer support division, just like HP, who are fully trained to deal with all of the year 2000 issues, and also have people in all of the Intel sales and marketing geographies around the world who are prepared to cover all these issues in detail as they come in on the 1–800 line system that our company has, just like HP's.

Mr. HORN. Mr. Willemssen, any more comments on that?

Anybody have any more questions you'd like to raise having heard all of your colleagues on the subject? Phone company we know is happy.

But anyhow, I just have one more and that gets back to your suppliers yet. I take it you've all done an inventory of your suppliers to see if anything would slow up. I don't know if you're using a Japanese inventory system where it's flowing into your assembly line on a steady basis.

Have you had any problems with suppliers being 2000 compliant?

Mr. WHITWORTH. We have at HP. In fact, one of our departments, the corporate procurement department that manages the relationship for some of the key suppliers that are common to a number of HP organizations made it a priority to first set up a survey to find out what our suppliers were doing. If they didn't get the answers that they were looking for, we would go and spend time and do in-depth interviews with some of our key suppliers.

We have in some instances moved from a single source supply to dual sourcing because we weren't comfortable with the conditions, and we also said some of the companies we were not comfortable with, we would eliminate from future possible business within HP. So we have made that sort of a condition for doing business with HP. But it hasn't been in a, let's call it a mean-spirited way. Part of our job is to get with that supplier and work with them to see if we can improve their own Y2K readiness following some of the patterns and some of the lessons that we've learned at HP. So we're trying the best we can to do that. It's being done all over the world, not just here in the United States, because our supply chain is everywhere.

And I'd say the general response we've gotten has been very, very positive from the suppliers. But that probably is the biggest degree of uncertainty, because each of those suppliers then in turn relies upon someone else who relies upon someone else, and it's very difficult from a corporate standpoint at HP to follow that chain all the way up and down and really take total ownership for guaranteeing the answers are right.

Mr. HORN. Mr. Hall, is that pretty much the way Intel has handled it?

Mr. RICHARD HALL. Yes. We've cut off some suppliers, not a large number, but we've stopped doing business with some. Before the end of the calendar year, there are more that we'll have to stop doing business with, and I doubt we will resume doing business with them, because the failure to address and manage the year 2000 problem is a demonstration of incompetence which would disqualify them from doing business with us in the future. It's unfortunate, but I think you're going to find this phenomenon accelerating very rapidly as the calendar goes by toward December.

Mr. HORN. It sort of surprises me when they've got major firms such as yours and HP that they wouldn't conform to assure you the supply source that they are. I would think what's doing? Have they got other customers that just don't care about it, or what would they do?

Mr. RICHARD HALL. I don't know the answer. I have the same question, and I don't know the answer.

Mr. HORN. Well, if we have any, I'd be fascinated by that, because I think it's a major problem down the line for all of you, and I'm glad you're on top of it.

That's all the questions I have on this subject. We might send a few to you afterwards, if you wouldn't mind just replying to us. We'll put in that objection at this point in the record.

I wish a good part of America tuned in and listened to this panel and the last panel, because I think they would have learned a lot. So I thank you all for coming out on a Saturday and not sailing or whatever you do on Saturdays, and thanks for coming.

We're down to panel three now.

Garth Hall, the manager of project 2000 is with the Pacific Gas & Electric Co.; Karen Lopez, division manager, administrative services, Silicon Valley Power; Dr. Frances E. Winslow, director, Office of Emergency Services, city of San Jose; William Lansdowne, chief of police, city of San Jose; John McMillan, deputy fire chief, city of San Jose.

Please come forward. I think you can see those signs. OK. We've got everyone behind the right sign. I see. If you don't mind, please stand up; raise your right hands.

[Witnesses affirmed.]

Mr. HORN. The clerk will note that all five witnesses affirmed.

And we will start with Mr. Hall. We're delighted to see him again. He was with us in our statewide hearing in Sacramento yesterday, and I notice your statement is even larger today. What did you do? Work all night? We didn't get the full version yesterday.

STATEMENTS OF GARTH HALL, MANAGER OF PROJECT 2000, PACIFIC GAS & ELECTRIC CO.; KAREN LOPEZ, DIVISION MANAGER, ADMINISTRATIVE SERVICES, SILICON VALLEY POWER; FRANCES E. WINSLOW, DIRECTOR, OFFICE OF EMERGENCY SERVICES, CITY OF SAN JOSE; WILLIAM LANSDOWNE, CHIEF OF POLICE, CITY OF SAN JOSE; AND JOHN McMILLAN, DEPUTY FIRE CHIEF, CITY OF SAN JOSE

Mr. HALL. Mr. Chairman, it is indeed a pleasure to be here again today on behalf of PG&E Corp. I oversee all of the companies within our nation-wide energy business, including the utility, which of course is a major area of interest today, and I can assure you again, as I did yesterday, that the standards for our Y2K readiness across all lines of business has been equally as high as it has been in the utility.

Our program, of course, had all the elements that have been discussed from the beginning of inventory all the way through contingency planning that I mentioned yesterday. We have been through all that process with all of our affiliates including the utility, and in July we were very pleased in the utility, PG&E, to inform the North American Electric Reliability Council which received a request from the Department of Energy to oversee the utilities nation wide in terms of their electrical reliability, in July we were pleased to report that all of our electric delivery systems are Y2K ready. That includes our hydro and our fossil power plants that we still own. And in addition to that, we have a handful of items left to test across our gas and nuclear energy arenas, and expect to achieve full compliance with those very soon, by September.

Even though we are very confident in our internal systems that I've just summarized, we're still taking our external dependencies very seriously. We have up to 2000 mission-critical business partners, suppliers and government agencies that we have identified, and have developed for each of those a contingency plan in case they fail to supply the service to us. Even though in almost all cases we have received very satisfactory responses back from them, and we have a fairly high degree of confidence based on that, and have had dialogue with them that they will be ready as well, we have still taken that precaution, because of social responsibility to provide high quality electric power and gas supply, to make sure that we have contingency plans in place to assure the public we will be ready.

At a higher level, as mentioned yesterday, we have performed two rounds of high-level business recovery drills, which is our customary practice to deal with storms, earthquakes and similar disasters, focussing now to make sure that the teams that would respond to those kinds of disasters, including the IT teams, are very well prepared to deal with any Y2K events, which, of course, we do not expect.

We also recognize, again, the importance of communicating to our customers and others our readiness, and we have met with over 100 external customer groups and have assured them and demonstrated our program, answered their questions about how they should interact with us, and have prepared everyone to be ready.

In fact, we will have, over the New Year's weekend, the transition period, we'll be elevated to the highest state of readiness we have within our capability, which is the level at which we deal with any major outage or any storm-related or earthquake outage. We will be at that level of deployment, ready for any emergency over the New Year weekend. That includes all of our distribution emergency centers, including those here in Santa Clara County. That's where we have our closest connection with emergency services of fire departments, police departments, and Offices of Emergency Services. Those connections will be well established.

We have also met with many customer groups, as I mentioned, Hewlett Packard, Wells Fargo, Catholic Healthcare West for example, Shell Oil, government agencies, city of Milpitas for example, Santa Clara County, also trade groups, for example the California League of Food Processing. All of these groups we have shared information with. They have, to our best knowledge, been very satisfied with that information, and we have opened opportunities for them to hear more if they need to. We have a website available at www.pge.com, which has a Y2K section with current status information and other information as well.

With that, I conclude my remarks. Thank you again.

Mr. HORN. Thank you.

[The prepared statement of Mr. Garth Hall follows:]

PG&E Corporation

One Market, Spear Tower
Suite 2400
San Francisco, CA 94105
415.267.7000
Fax: 415.267.7268

Testimony of Garth Hall

Program Manager, Y2K Program Management Office

PG&E Corporation

before

THE GOVERNMENT MANAGEMENT, INFORMATION AND

TECHNOLOGY SUBCOMMITTEE

OF THE HOUSE COMMITTEE ON GOVERNMENT REFORM

August 14, 1999

San Jose City Hall
San Jose, California

PG&E Energy Services, PG&E Energy Trading, PG&E Gas Transmission, and PG&E Generating are not the same companies as Pacific Gas and Electric Company, the utility, and are not regulated by the California Public Utilities Commission. Customers of Pacific Gas and Electric Company do not have to purchase products or services from these companies to receive quality service from Pacific Gas and Electric Company.

Year 2000 Readiness Disclosure

Good Morning, Mr. Chairman and Members of the Subcommittee. I am Garth Hall, Program Manager of the Y2K Corporate Program Office of PG&E Corporation. My office oversees and coordinates the Y2K efforts of all the Corporation's lines of business: Pacific Gas and Electric Company, the utility, PG&E Gas Transmission, PG&E Energy Services, PG&E Energy Trading and PG&E Generating. Thank you for giving me this opportunity to tell you about our program and its progress, and to support your efforts regarding the important issue of Y2K readiness. While the primary focus of this presentation will be on the utility, the same success story is true for our other lines of business.

I can assure you that we are taking Y2K seriously. We began our Y2K efforts in 1996. Since then, we have been working hard and committing the necessary resources toward resolving this issue.

Our goal is to have our mission-critical systems Y2K ready before the end of this year, and we are on target to do just that. As you probably know, the Department of Energy has asked the North American Electric Reliability Council, or NERC, to oversee the Y2K efforts of the nation's electric utilities to ensure electric reliability is maintained. Last month, our utility unit, Pacific Gas and Electric Company, reported that it is Y2K ready to NERC. Beyond reports to NERC, we also report the status of our nuclear systems to the Nuclear Regulatory Commission and Nuclear Energy Institute, and we respond to surveys about our gas systems to the American Gas Association. In NERC's final report, issued last week, NERC said it believes that "the electric power industry will operate reliably into the Year 2000."

We echo that sentiment throughout PG&E Corporation, and fully expect January 1, 2000 to be a day like any other day. To date, we have not found any Y2K problems that we have not been able to resolve. That being said, I also want to assure you that we fully understand the need to be prepared. Being prepared is at the core of our business – whether it is for storms, fires, earthquakes or Y2K. We are developing and testing comprehensive contingency plans. And we will continue various kinds of validation and quality assurance efforts into the new century to minimize the risk of interruptions of service for our customers.

Before taking your questions, I would like to briefly describe our Y2K program, contingency plans, and our public outreach program. We are addressing Y2K problems found in (1) software developed by our lines of business for specific applications, (2) software provided by vendors, (3) computer hardware and (4) embedded electronic systems. The first step of our program was to compile an inventory of all systems used, and to assess which systems are mission-critical. We purposefully concentrated our efforts on those systems that directly affect our safety and reliability, customers, products, and revenue. The utility depends on these mission-critical systems to deliver gas and electricity reliably and safely. Examples are those systems that provide outage information and monitor the transmission of gas and electricity, safety-related systems at our generating plants, customer billing and metering, and computer and telecommunications infrastructure that supports business operations.

Our plan calls for the remediation of any mission-critical system not Y2K ready. Remediation means that a system is either repaired, replaced or retired. After remediation, testing is performed to verify that the system will continue to operate into the next millennium. Certification, or the final step in our process, is to officially acknowledge that the work has been completed appropriately. Certification requires a review and formal sign-off by an officer of the company.

Another important component of our Y2K plan addresses mission-critical business relationships consisting of partners, suppliers and government agencies. We have assessed these relationships using Y2K compliance information obtained from them and, based partly on this information, have developed contingency plans for all of them.

We depend on these relationships, and if any of them experience Y2K problems, the reliability of our services may be affected. Indeed, the reliability of the entire electric industry hinges on its many interconnections and interdependencies. For example, to deliver power to utility customers, we are dependent upon the California Independent System Operator (ISO), which is located in Folsom. The ISO controls the operation of the State's electrical transmission system. The ISO is in turn dependent upon the proper operation of various transmission systems it is connected to throughout the western part of the US and Canada. Also, the utility sells to and buys power from the California Power Exchange, which relies on other many other power plants that must function properly to provide power needed at any time.

With the complexity of our industry and the physical nature of our utility system, it only makes sense to prepare for the unexpected. We are experienced in planning for contingencies; it's important to our business and service. Every year we prepare for the possibility of fires in the summer, heavy storms in the winter, and earthquakes that could occur at any time. We participate in emergency drills internally and with external agencies. We have existing plans and procedures in place for dealing with emergencies involving our gas, electrical, generating and trading systems.

We are building on these existing emergency plans in preparation for problems that may result from Y2K. We have been testing our plans and will continue to do so throughout the year. We are performing tabletop exercises with key personnel and training designated employees. In addition, under the direction of NERC, we participated with the ISO and other utilities in a nationwide Y2K exercise in April 1999 and will take part in a second exercise scheduled for September 1999.

Utility contingency plans for the Y2K roll-over period include: extra staffing at many of our facilities, operation of additional 24-hour call centers, emergency centers staffed and operational, and pre-scheduled transmission of additional gas and electricity. If gas or electric service interruptions occur, we will have personnel on hand to restore service as quickly and safely as possible.

We are committed to informing our customers and business partners about our Y2K plans, progress and contingency planning. We have a number of different avenues to communicate–from our regularly-updated Internet web sites and customer newsletters to face-to-face meetings.

At our utility, we have responded by letter to more than 3,400 customer inquiries. Since February of this year, we have averaged more than 9,000 hits each month on our utility web site. Our media representatives have conducted nearly 250 interviews on this issue. Utility governmental relations representatives have kept elected officials apprised of our program.

The utility has taken part in more than 160 presentations throughout the service area, from San Francisco to the Sierra foothills, and from Redding to Bakersfield. Our audiences for these presentations have run the gamut - from corporations, such as Hewlett Packard, Wells Fargo, Catholic Healthcare West and Shell Oil, to government agencies, such as the City of Milpitas, Santa Clara County, and power and water agencies; and from trade groups, like the California League of Food Processors, to conference groups such as the Year 2000 Expo in San Jose.

In closing, we feel we have implemented a strong and effective plan, devoted appropriate resources and diligently monitored the Y2K work throughout the Corporation. Though no one is able to predict with certainty what the Y2K transition will bring, we will be ready.

Thank you, Mr. Chairman, for inviting me to participate today, and I would be pleased to answer your questions.

Mr. HORN. We now have Karen Lopez the division manager, administrative services for Silicon Valley Power.

Ms. LOPEZ. Mr. Chairman, thank you for inviting the city of Santa Clara's Electric Utility, Silicon Valley Power, to address you today on the year 2000 readiness.

Mr. HORN. Do you want to move that right in front of you. Mics are difficult nationwide.

Ms. LOPEZ. I usually don't have a problem with speaking too loudly, so we'll try that.

My name is Karen Lopez. I am the division manager for the administrative services for Silicon Valley Power, and I'm also our year 2000 project team leader. I would first like to tell you a little bit about Silicon Valley Power.

Silicon Valley Power is the municipal electric utility for the city of Santa Clara. As you heard earlier from Mr. Ron Garratt, our assistant city manager, Santa Clara is a charter city located in the heart of Silicon Valley. The city offers electricity and energy services through the trademarked name of Silicon Valley Power. Since 1896, the city has provided electric service to the businesses and citizens within its boundaries. Santa Clara has an estimated population of 103,000 people. At the end of December 1998, Silicon Valley Power served approximately 46,500 customers, and had a total sales of 2,506 GWh with a peak demand of 443.8 MW. Almost 87 percent of Silicon Valley Power's energy sales are made to industrial customers such as Intel, 3COM, Sun Microsystems and other internationally known corporations.

To provide electric services within its service area, Silicon Valley Power owns and operates generation, transmission and distribution facilities. Silicon Valley Power also purchases power and transmission services from others, and participates in several joint power agencies with other municipalities.

Silicon Valley Power has a year 2000 readiness project plan that articulates the steps that we have taken over the past several years to be ready to maintain a reliable supply of power to our customers into the next millennium. As a part of this plan, Silicon Valley Power formed a project team consisting of representatives from each of our divisions to coordinate our activities. The project team has established milestones, assigned responsibilities and monitors our progress toward minimizing the year 2000 risks to our customers and to our continued reliable supply of services to those customers.

Silicon Valley Power internally inventoried and assessed all computing systems, equipment and software, for year 2000 readiness. We also contracted with an external vendor for the inventory and assessment of all other Silicon Valley Power equipment for potential year 2000 risks from embedded systems. That inventory and assessment were both completed in 1998 and continue to be updated as changes occur.

Silicon Valley Power has not identified any internal system critical to our supply of electrical service to our customers that is not year 2000 ready. All of our business critical and non-critical systems and equipment either have been remediated or are in the process of being remediated. This process is expected to be completed before September 1st. The testing of all systems capable of being tested without impact to our customers will also be completed by September 1st. Due to the constant demand of supply of electricity to our customers, it is not fully possible to test all of our equipment without disruption of that supply. However, let me say again, that Silicon Valley Power has not identified any non-year 2000 ready system or equipment that is critical to our ability to supply electricity to our customers.

The amount of dollars that Silicon Valley Power has and plans to expend in total on our year 2000 readiness efforts has not been formally developed, since year 2000 concerns have been incorporated into our technology projects over the past several years. However, since those concerns, or those technology projects and concerns were not exclusive drivers to these projects, a breakdown of costs that relate directly to the year 2000 would be extremely difficult to perform.

Our staff has met with all of our business partners regarding their and our year 2000 readiness efforts. We send representatives to and participate in the year 2000 readiness meetings of various agencies including the Western Area Power Agency, the Northern California Power Agency, the North American Electric Reliability Council, the California Municipal Utilities Agency, and the Independent Systems Operators.

Although there are no plans at this time for Silicon Valley Power to be a formal participant in interagency testing, Silicon Valley Power has, and will continue, to monitor the year 2000 readiness activities of our partners, suppliers, vendors and customers for any potential impact on our ability to continue to supply those services to our customers. Silicon Valley Power will remain vigilant in this area.

For over 100 years Silicon Valley Power has provided a reliable supply of electrical services to our customers. During this time, the city of Santa Clara has experienced several major natural disasters such as floods and earthquakes. From these experiences we have developed contingency plans and emergency plans to minimize any external impact on our ability to continue to provide electrical services. In addition, we are in the process of developing year 2000 specific contingency plans. On April 9th, in conjunction with the North American Electric Reliability Council's drill, Silicon Valley Power conducted an internal year 2000 readiness contingency planning drill with representatives from all Silicon Valley divisions, power divisions, and several other city departments such as our Fire and Police. We will also hold a year 2000 rollover staffing simulation and readiness preparation exercise on September 9th, concurrent with the planned North American Electric Reliability Council drill.

Silicon Valley Power has been extremely active in its efforts to educate and to communicate regarding our concerns and efforts for year 2000 readiness. We have held educational meetings with all Silicon Valley Power staff, with our major industrial customers, both individually and in groups, with our commercial or small business customers, our residential customers and through our City Council. Future meetings are scheduled with each of these groups to not only continue our educational efforts, but to provide informational updates on our year 2000 readiness status.

In closing, I want to thank the committee for the opportunity to be here today, and on behalf of the city of Santa Clara's City Council, I want to extend our appreciation to this committee for its efforts in trying to look at this throughout the Nation.

Mr. HORN. Well, thank you very much, Ms. Lopez.

[The prepared statement of Ms. Lopez follows:]

Year 2000 Readiness

Congress of the United States

House of Representatives
August 14, 1999

Committee on Government Reform
Subcommittee on Government Management, Information, and Technology

Efforts of State and Local Governments
And Businesses to
Address the Year 2000 Computer Problem

Testimony of
Karen Lopez
Division Manager
Silicon Valley Power
City of Santa Clara

Silicon Valley Power
CITY OF SANTA CLARA

Biography of

KAREN E. LOPEZ
DIVISION MANAGER–ADMINISTRATIVE SERVICES
CITY OF SANTA CLARA'S ELECTRIC UTILITY, SILICON VALLEY POWER

Karen Lopez has been with the City of Santa Clara's Electric Utility, Silicon Valley Power since 1997 as Division Manager-Administrative Services. Previously Karen served for eight years as the Communications Systems Manager for the City of Sunnyvale where her responsibilities included the daily operations, administration and policy development for internal and external voice, data, and video communication systems within the city.

Karen's responsibilities include the administration of departmental budgeting, information technology, personnel issues, contracts, procurements, and special projects.

Karen holds a Bachelor of Science degree in Information Systems Management from the University of San Francisco and a Masters degree in Business Administration from San Jose State University.

Silicon
Valley
Power
CITY OF SANTA CLARA

Giving you the power

to change the world.

August 13, 1999

Stephen Horn, Chairman
Subcommittee on Government Management,
Information, and Technology
Congress of the United States
2157 Rayburn House Office Building
Washington, DC 20515-6143

Subject: Presentation on Year 2000 Readiness

Dear Chairman Horn and Committee Members:

Mr. Chairman and members of the Subcommittee, thank you for inviting me today to speak on the subject of Year 2000 Readiness in Silicon Valley Power, City of Santa Clara Electric Utility. My name is Karen Lopez, Division Manager for Administrative Services for Silicon Valley Power.

Thank you for inviting City of Santa Clara's Electric Utility – Silicon Valley Power to address you today on Year 2000 Readiness. I would like to briefly acquaint you with Silicon Valley Power.

Who is Silicon Valley Power?

Silicon Valley Power (SVP) is the municipal electric utility for the City of Santa Clara. As you heard earlier, from Mr. Ron Garratt, our Assistant City Manager, Santa Clara is a charter city located in the heart of Silicon Valley. The City has determined to offer its electricity and energy services through the trademarked name of "Silicon Valley Power." Since 1896, the City has provided electric service to the businesses and citizens within its boundaries. In 1997, the City had an estimated population of approximately 100,000. At the end of December 1998, SVP served approximately 46,500, had total sales of 2,506 GWh and a peak demand of 443.8 MW. Approximately 87.4% of SVP's energy sales are made to industrial customers, such as, Intel, 3COM, Sun Microsystems and other internationally known industrial customers.

500 Warburton Ave.

Santa Clara, CA 95050

Ph: (408) 261-5292

Fax: (408) 249-0217

SVP staff has met with all of SVP's business partners regarding their, and our, Year 2000 Readiness efforts. SVP sends representatives to and participates in the Year 2000 Readiness meetings of various agencies including Western Area Power Agency (WAPA), Northern California Power Agency (NCPA), North American Electric Reliability Council (NERC), California Municipal Utilities Agency (CMUA), and the Independent Systems Operators (ISO).

Although there are no plans at this time for SVP to be a formal participant in interagency testing, SVP has, and will continue to, monitor the Year 2000 Readiness activities of our partners, suppliers, vendors and customers for any potential impact on our ability to supply services to our customers. SVP will remain vigilant in this area.

Contingency Plan if Things Go Wrong.

For over 100 years, SVP has provided a reliable supply of electrical services to our customers. During this time, the City of Santa Clara has experienced several major natural disasters; such as, floods and earthquakes. From these experiences, SVP has developed emergency plans to minimize external impacts on its ability to continue to provide electrical service. In addition, we are in the process of developing Year 2000 specific contingency plans. On April 9, in conjunction with the North America Electrical Reliability Council's (NERC) drill, SVP conducted a Year 2000 Readiness contingency planning drill with representatives from all SVP divisions and several other City departments. We will also hold a Year 2000 rollover staffing simulation and Readiness preparation exercise on September 9, 1999, concurrent with the planned NERC drill.

Communications.

SVP has been extremely active in its efforts to educate and communicate regarding its concerns and efforts for Year 2000 Readiness. SVP has held educational meetings with all SVP staff, with our major industrial customers, both individually and as a group, and with our City Council. Future meetings are planned with our commercial customers, industrial customers, SVP staff, and the citizens of Santa Clara. These meetings will be used to not only continue our educational efforts, but to provide information updates on SVP's Year 2000 Readiness status.

In the packet that we have provided you is a sample of the documents that we have distributed and/or made available to our customers or that represent SVP's Year 2000 Readiness activities. They include the following:

Stephen Horn, Chairman
Subcommittee on Government Management,
Information, and Technology
Subject: Presentation on Year 2000 Readiness
August 13, 1999
Page 4

Sample Documents of Materials Distributed to Customers.

"Personal Y2K Checklist" - Checklist available to all customers and distributed at commercial and residential customer meetings. (Exhibit A)

"SVP's Year 2000 Readiness Project Update" - copy of presentation at commercial customer meeting on July 16, 1999. (Exhibit B)

"SVP Year 2000 Project Guidelines" - Internal listing of project tasks, their description and status. (Exhibit C)

"Y2K" - General information available to all customers and distributed at commercial and residential customer meetings. (Exhibit D)

"San Jose Mercury News Survey Response" - Response to San Jose Mercury Newspaper's questions on SVP's Year 2000 activities. (Exhibit E)

"Risk Assessment-Contingency PlanR2" - Spreadsheet listing potential Year 2000 risks, their description, probability, impact on SVP, and strategies to prevent or mitigate their occurrence. (Exhibit F)

"Major Customer Y2K Survey" - Survey distributed to SVP's major customers to obtain information regarding their Year 2000 activities and potential impact to SVP. (Exhibit G)

"Electric Utility Y2K Links" - Listing of recommended internet sites for information on the power supply and the Year 2000. (Exhibit H)

"Year 2000 Activities Checklist" - Checklist to assist commercial and small business customers in their Year 2000 Readiness activities. (Exhibit I)

In closing, I want to thank the Committee for this opportunity to speak. On behalf of the City Council of the City of Santa Clara, I extend our appreciation to the Committee for your diligence and efforts in determining Year 2000 Readiness throughout this nation.

Personal Y2K Checklist

Things to do before January 1, 2000:

✓ Make backup copies of important files on your home and office computers.

✓ Obtain current copies of bank statements, mortgage schedules and other financial accounts.

✓ Refill prescription medications.

✓ Stay healthy and don't schedule any major operations.

✓ Stock up on groceries and other basic supplies.

✓ Have a good supply of flashlights, batteries, candles, matches, kerosene lamps and kerosene on hand.

✓ If you have a wood stove, top off your wood supply.

✓ Some juice or milk jugs and fill them with water – especially if you depend on a well which in turn is dependent on an electric pump.

✓ Have some cash on hand in case the ATM machine freezes up or your credit cards come back as "account unknown" – but don't panic and cause a run on the banks!

✓ Top off the gas tanks on your vehicles.

✓ Do your laundry.

✓ Spend New Year's Eve at home or with nearby family and friends; if you do go some place for the holidays, be prepared to stay a while.

EXHIBIT A

Basic Supplies

The following are recommended basics for each family.

Food

□ Ready-to-eat canned meats, fruits and vegetables

□ Canned juices, milk, soup (if powdered, store extra water)

□ Staples—sugar and pepper

□ Ready-to-eat cereals and uncooked instant cereals (in metal containers)

□ Dry, crisp crackers (in metal container)

□ Potatoes (fresh or dried flakes)

□ Foods for elderly or persons on special diets

□ Comfort/stress foods (cookies, hard candy, sweetened breakfast cereals, lollipops, soda pop, instant coffee, tea bags, cocoa, chocolate bars, canned nuts, etc.)

□ High energy foods—peanut butter, jelly, crackers, granola bars, trail mix

□ Dried spices (choose the spices your family likes, i.e. garlic, onion, oregano, chili powder, etc.)

□ Juices (canned or powdered, Kool-Aid)

□ Vitamins and supplements (basic)

□ Baking powder

□ Beans

□ White rice

□ Non-carbonated soft drinks

□ Bouillon products (beef & chicken)

□ Vegetable oils

□ Dry Pasta (spaghetti, macaroni, lasagna, etc)

EXHIBIT A

Miscellaneous Supplies

- □ Mess kits, or paper cups, plates and plastic utensils (you don't want to waste drinking water washing dishes!)
- □ Can Opener (no electricity required)
- □ Flashlights with Extra Batteries
- □ Swiss Army Knife
- □ Multi-Purpose Tool Box
- □ Matches & Lighters (some waterproof/windproof)
- □ Candles and Oil Lamps
- □ Chemical Light Sticks
- □ Fire Extinguisher
- □ Rope
- □ Aluminum Foil
- □ Plastic Buckets (plenty of extra buckets on hand)
- □ Sewing Kit (needles, thread, scissors, etc)
- □ Smoke Alarms (Extra Batteries)
- □ Shut-off Wrenches (Water, Gas, etc.)
- □ Baby Supplies (bottles, disposable bottle liners, wipes, diapers, ointments, etc.)
- □ Rolls of Plastic Sheeting (solar stills, shelter, roof leak repair, many uses)
- □ Toilet Paper
- □ Hygiene Supplies (toothpaste & brushes, floss, deodorant, razors, shave cream, hydrogen peroxide, shampoo, etc.)
- □ Feminine Hygiene Supplies (may want to consider The Keeper)
- □ Cleaning Supplies (soap, detergents, disinfectants, chlorine bleach, garbage bags)

EXHIBIT A

- □ Extra Personal Items (contacts & solution, eyeglasses, dentures, retainers,
- □ Pet supplies (food, litter, vaccines, etc.)

Communications

- □ CB Radio/walkie-talkies
- □ Radio Frequency Scanners
- □ AM/FM radio with weather band (battery Operated) (High powered reception)(Plenty of extra Batteries)

Medical

- □ First Aid Kit
- □ syrup of ipecac
- □ Band-Aids - assorted sizes
- □ nylon or paper tape
- □ butterfly bandages (3 - make with 1 " adhesive tape)
- □ adhesive tape - 1" wide
- □ gauze - 2" wide
- □ cotton - tipped swabs
- □ telfa sterile pads (4)
- □ gauze sterile pads 4"x4" (10)
- □ sterile eye pads (2)
- □ magnifying glass (remove splinters ~ dirt in eyes)
- □ tweezers
- □ flashlight (light outage ~ check pupils)
- □ needle (remove splinters)
- □ antibacterial ointment (bacitracin ingredient)

EXHIBIT A

□ sharp, blunt end scissors

□ ammonia inhalant (fainting)

□ calamine lotion (insect bites, poison iv)1

□ children's aspirin & liquid acetaminophen - only as directed by a physician

□ petroleum jelly (helps prevent nosebleeds, lubricate thermometer)

□ hydrogen peroxide (cleans wounds after initial cleansing, keep away from eyes)

□ iodized salt (heat exhaustion, ltsp. Salt in qt. Water)

□ ace bandage (3" wide)

□ safety pins

□ thermometer (rectal for under 4 years of age)

□ large clean cloth (to restrain child or for burns)

□ tape measure (length of wounds)

□ rubbing alcohol (remove ticks)

□ bar soap, non-perfumed

□ insect kit (if history of severe allergies)

□ baking soda (soothes insect bites)

□ Special Equipment (if anyone has special equipment needs gear up)

□ Special Conditions (if anyone has special conditions gear up on supplies)

□ Prescriptions (see if your Doctor will write up extra prescriptions?)

Water

□ Water Storage Containers (1,5,55 gallon etc.)

□ Water Filters / Purification Systems

□ Water Purification Tablets

EXHIBIT A

□ Bleach for Water Purification

□ Solar Water Stills

Other

□ Cash (one month supply)

□ Batteries - (plenty of extra batteries for everything you can think of)

□ Wood Burning Stove

□ Kerosene Heaters

□ Warming Pads for hand/body

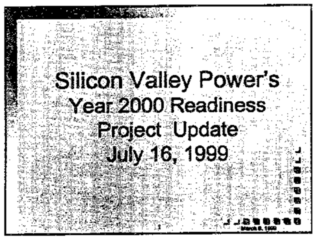
□ Other Alternate Heat Sources (battery powered carbon monoxide detector)

□ Extra blankets & sleeping bags and winter clothing

□ Dogs are a good heat source

□ Anything else you can think of that you might need or want!

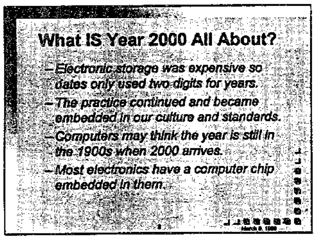
EXHIBIT A



Silicon Valley Power's
Year 2000 Readiness
Project Update
July 16, 1999

1

March 8, 1999

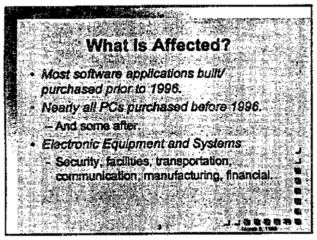


What IS Year 2000 All About?

- *Electronic storage was expensive so dates only used two digits for years.*
- *The practice continued and became embedded in our culture and standards.*
- *Computers may think the year is still in the 1900s when 2000 arrives.*
- *Most electronics have a computer chip embedded in them.*

2

March 8, 1999



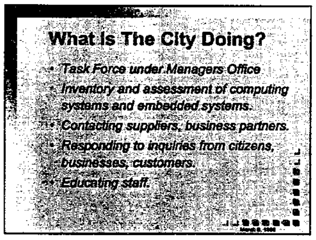
What Is Affected?

- *Most software applications built/ purchased prior to 1996.*
- *Nearly all PCs purchased before 1996.*
  - And some after.
- *Electronic Equipment and Systems*
  - Security, facilities, transportation, communication, manufacturing, financial.

3

March 8, 1999

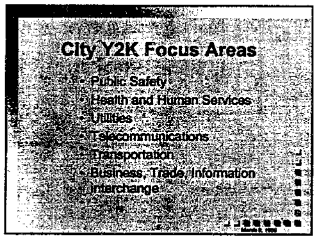
EXHIBIT B



What Is The City Doing?

- *Task Force under Managers Office*
- *Inventory and assessment of computing systems and embedded systems.*
- *Contacting suppliers, business partners.*
- *Responding to inquiries from citizens, businesses, customers.*
- *Educating staff.*

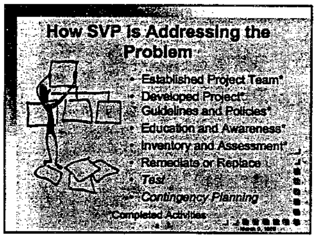
March 8, 1999



City Y2K Focus Areas

- Public Safety
- Health and Human Services
- Utilities
- Telecommunications
- Transportation
- Business, Trade, Information Interchange

March 8, 1999



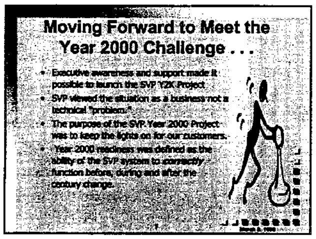
How SVP Is Addressing the Problem

- Established Project Team*
- Developed Project*
- Guidelines and Policies*
- Education and Awareness*
- Inventory and Assessment*
- Remediate or Replace
- *Test*
- *Contingency Planning*

*Completed Activities

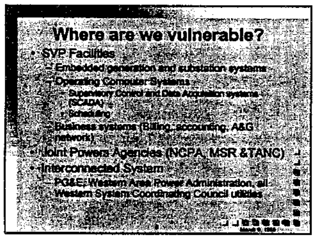
March 8, 1999

EXHIBIT B



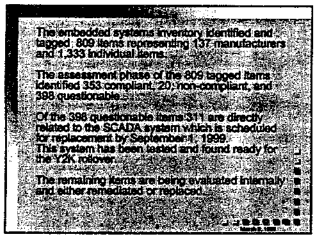
Moving Forward to Meet the Year 2000 Challenge . . .

- Executive awareness and support made it possible to launch the SVP Y2K Project
- SVP viewed the situation as a business not a technical "problem."
- The purpose of the SVP Year 2000 Project was to keep the lights on for our customers.
- Year 2000 readiness was defined as the ability of the SVP system to *correctly* function before, during and after the century change.



Where are we vulnerable?

- SVP Facilities
  - Embedded generation and substation systems
  - Operating Computer Systems
    - Supervisory Control and Data Acquisition systems (SCADA)
    - Scheduling
  - Business systems (Billing, accounting, A&G network)
- Joint Powers Agencies (NCPA, MSR &TANC)
- Interconnected System
  - PG&E, Western Area Power Administration, all Western System Coordinating Council utilities



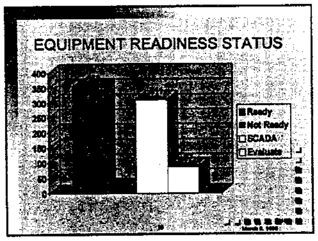
The embedded systems inventory identified and tagged 809 items representing 137 manufacturers and 1,333 individual items.

The assessment phase of the 809 tagged items identified 353 compliant, 20, non-compliant, and 398 questionable.

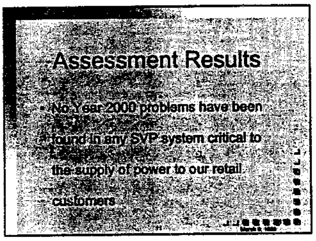
Of the 398 questionable items 311 are directly related to the SCADA system which is scheduled for replacement by September 1, 1999.
This system has been tested and found ready for the Y2K rollover.

The remaining items are being evaluated internally and either remediated or replaced.

EXHIBIT B

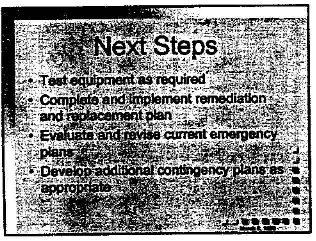


EQUIPMENT READINESS STATUS



Assessment Results

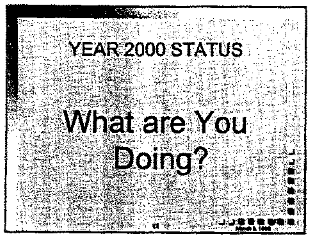
- No Year 2000 problems have been found in any SVP system critical to the supply of power to our retail customers



Next Steps

- Test equipment as required
- Complete and implement remediation and replacement plan
- Evaluate and revise current emergency plans
- Develop additional contingency plans as appropriate

EXHIBIT B



YEAR 2000 STATUS

What are You Doing?

EXHIBIT E

SVP . _AR 2000 PROJECT GUIDELINES

8/10/99

	Task	Sub-Task	Sub-Task	Description	Status
Project Management					
	Project, General				
		Establish Scope of the Project		Determine what is to be included in the project and what is to be excluded. Determine the high level requirements and relate them to the business objectives. Record the assumptions.	Complete
		Develop Policies, guidelines and		Develop and implement needed policies, guidelines and procedures to manage project.	Complete
			Desktops		Complete
			Embedded Systems		Complete
			Project Overview		Complete
			New Equipment		Complete
			New software		Complete
			Date format standard		Complete
			Determine vulnerable dates		Complete
			Define Y2K Readiness		Complete
		Develop and document a high-level Year 2000 strategy		A high-level Year 2000 strategy provides SVP's executive management with a roadmap for achieving Year 2000 compliance. The strategy will discuss key Year 2000 issues, including the program's management structure, reporting requirements, and initial cost and schedule estimates.	Complete
		Obtain and formalize executive		The management support for the agency's Year 2000 strategy should be formalized.	Complete
		Develop Year 2000 program plan and tracking.		Including schedules for all tasks and phases of the Year 2000 program, master inventory and assessment of systems and their components, assignments and responsibilities, risk assessment, and contingency plans for all systems.	Complete
		Identify, prioritize, and mobilize needed resources		Achieving Year 2000 compliance will require significant investment in two vital resources--money and people. Accordingly, SVP will need to make informed choices about priorities within the organization by assessing the costs, benefits, and risks of competing projects. In some instances, SVP may have to defer or cancel new system development efforts and reprogram the freed resources to achieve Year 2000 compliance.	On Going
		Develop Project Plan and Time Schedule		Determine constraints. Determine activities required. Estimate effort and duration. Identify resources.	Complete
			Maintain Project Plan and Time Schedule	Update the schedule. Document assumptions.	On Going
		Project Organization		SVP's Year 2000 program--headed by a program manager--should be adequately staffed to ensure the successful completion of the assessment phase. In addition to technical skills, the program team should be able to track the cost and schedule for Year 2000. Select and prepare the people whose involvement will be necessary for the project to succeed.	Complete
			Establish Year 2000 executive management council	Identify the senior management team who will direct and be accountable for the projects success. Document the responsibilities to be performed. A committee or a council needs to be established within the agency to continually coordinate with the programmatic and functional area managers on priorities and potential mission impact if certain processes and systems malfunction. A process for quick conflict resolution on priorities between programmatic and functional areas is also needed.	Complete
			Identify Project Manager	Identify the manager for this stage of the project. Document the responsibilities to be performed.	Complete

EXHIBIT C

SVP ', _AR 2000 PROJECT GUIDELINES

8/10/99

			Identify Project Team	Identify the people who are critical to the success of the project. Document the responsibilities to be performed.	Complete
			Identify Key Resources	Identify additional business or technical resources and liaisons required to support the project for business areas and major systems. Document the responsibilities to be performed.	Complete
			Determine Training Requirements	Assess the capabilities and skills of the project team. Establish a training plan to acquaint the project team with the methodologies, technologies, and business area under study.	Complete
	Risk Management				On Going
		Define the Year 2000 problem and its potential impact on the enterprise		Developing and publishing a high-level assessment of the Year 2000 issue provides executive management and staff with a high-level overview of the potential impact of the Year 2000 problem on the enterprise.	Complete
		Triage systems and equipment.		Identify criticality of all systems and equipment to success of SVP goals.	Complete
			Mission Critical	Must have to meet SVP goals.	Complete
			Necessary	Required, but alternate accommodation can be made.	Complete
			Useful	Convenient but not major disruption	Complete
			Irrelevant		Complete
		Create risk decision table		Define criteria for assigning and identifying risk tolerance	Complete
		Analyze Risks		Determine the risks associated with the project.	Complete
		Determine probability of risks		Identify for all systems and equipment	Complete
		Define acceptable risks			On Going
	Program management processes.			Monitor Year 2000 project, and ensure that project follows required policies and procedures.	On Going
		Maintain Project Schedule		Monitor and control the progress on the project.	On Going
			Manage Staff Assignments		Complete
			Develop and monitor change process	Update schedules with actuals. Reassess cost and completion dates.	On Going
		Produce Monthly Status Reports		Review and record the effort expended against the schedule. Review estimate to complete. Review status of project control documents. Decide if any corrective actions are needed. If required, adjust schedule by adding tasks and resources. Report to Management.	On Going
			Develop Reporting Forms		Complete
		Import/implement best practices			On Going
	Develop Budget				Complete
		Determine Project Costs		Ensure all project costs have been identified and are in the project budget.	Complete
	Schedule and Conduct Task Force Meetings				On Going
	Coordinate legal aspects with City Attny			Access to legal advice is a necessity.	On Going
	Document Control			Collect and maintain careful documentation on project to ensure proper coordination and establish records of efforts that could be vital in case of litigation.	On Going
		Contracts			On Going
		Readiness letters- sent			On Going
		Readiness letters-received			On Going
		Vendor responses			On Going
		Test results			On Going
		External contacts		Maintain information on the Y2K status of customers, suppliers, partners, and trading partners.	On Going
		Storage		Hard Copy and electronic copies.	Complete
	Develop Post Y2K clean-up plan				

EXHIBIT C

SVP . _AR 2000 PROJECT GUIDELINES

8/10/99

	Conduct Post Project Review				
Awareness				It is essential that executive management be fully aware of the Year 2000 problem and its potential impact on the electric utilities and its customers. It is the responsibility of the Y2k Project Manager to provide the leadership in defining and explaining the importance of achieving Year 2000 compliance, selecting the overall approach for structuring the agency's Year 2000 program, assessing the adequacy of the existing infrastructure to adequately support the Year 2000 efforts, and mobilizing needed resources.	**Complete**
	Establish an Understanding of the Y2K Problem			Essentially, the problem relates to the use of a 2 digit year used as a default year Number. Dates from and inc. Year 2000 will require a 4 digit field for all years 1900 forwards etc. The problem is not confined to software, but hardware also.	**Complete**
	Conduct a Year 2000 awareness campaign			A year 2000 awareness campaign is an important first step to raise the awareness of executive management and line staff about the potential impact of the Year 2000 problem on SVP's operations.	**On Going**
		Develop Internet Website		Part of City Website	**Complete**
			Maintain Website		**On Going**
		Establish internal information resources			**Complete**
			Intranet		**Complete**
			Library		**Complete**
			Quarterly Staff Presentations		**On Going**
	View Relevant Web Sites/Other Information			A list of web sites is available for reference.	**Complete**
Assessment				Organizations, including SVP, may not have enough resources, skill, or time to repair or replace all of their potential Y2k impacted systems. SVP will determine what systems are mission-critical and must be repaired or replaced, what systems support important functions and should be repaired or replaced, and what systems support marginal functions, and may be repaired or replaced later. The Year 2000 problem is not just an information technology problem, but is primarily a business problem. Thus, the process of identifying and ranking systems should not be limited to a simple inventory of applications and platforms, but must include assessments of the impact of all systems' failures on the agency's core areas and processes. The assessment will also include systems using information technology which operate outside the traditional information resource area, including utilities infrastructure systems and equipment.	**On Going**
	Conduct an enterprise-wide inventory of equipment & systems.			An enterprise-wide inventory of information systems and their components provides the necessary foundation for Year 2000 program planning. A thorough inventory ensures that all systems are identified and linked to a specific business area or process.	**Complete**
		IT Infrastructure			**Complete**
			Identified IT related projects		**Complete**
			Identify Hardware	Not only Computer hardware also other equipment and systems which may be time/date locked.	**Complete**
			Identify Software	Not only Computer software and data bases which may be time/date locked.	**Complete**
			Examine h/w and s/w for compliance		**Complete**
			Coordinate PCs		**Complete**

EXHIBIT C

SVP YEAR 2000 PROJECT GUIDELINES

8/10/99

		Embedded Systems			Complete
			Coordinate control systems		Complete
	Triage Systems			Assess systems and equipment based on defined criticality.	Complete
		Focus on core business critical areas and processes and develop a Year 2000 assessment document		All systems are not created equal. Systems supporting mission-critical processes are clearly more important than systems supporting mission support functions--usually administrative--although these are necessary functions. A focus on core business areas and processes is essential to the task of assessing the impact of the Year 2000 problem on SVP and for establishing the priorities for the year 2000 program.	Complete
		Assess the severity of potential Year 2000-induced failures		An assessment of the severity of Year 2000 failure needs to be done for each core business area and associated processes.	Complete
		Use inventory data to develop a comprehensive automated system portfolio and identify interfaces.		For each system identify links to core business areas or processes, platforms, languages, and database management systems, operating system software and utilities, internal and external interfaces, owners, the availability and adequacy of source code and associated documentation, and any other necessary characteristics for successful operation.	Complete
		Identify fixes.		Identify for each system or component the fix necessary (if any) and any replacement resources required .	Complete
			Distribution devices/systems which are service critical		Complete
			Microprocessor controlled with clock/calendar function		Complete
			Y2K problematic devices/systems have already been identified		Complete
			Which contain a a bug that leads to a "fatal" error?		Complete
			Which have a bug that will cause an immediate service interruption or inadvertent switching operation?		Complete
			Could any of these devices/systems fail without any immediate indications?		Complete
			How can specific problematic devices/systems be clearly identified (version, serial, and model numbers?)		Complete

EXHIBIT C

SVP ٫ _AR 2000 PROJECT GUIDELINES

8/10/99

		Prioritize system conversions and replacements		SVP must determine priorities for repairs and replacement by ranking based on key factors, such as business impact and the anticipated failure data. Also identify any equipment, application, database, archive, or interface that cannot be made ready because of resource and time constraints.	Complete
				Eliminate devices from inventory that do not contain internal date clocks or require date information for communications, i.e., device manuals, device displays.	In Process
	Interface Management			Analyze, fix, and test among internal projects and with external organizations.	In Process
		Address interface and data exchange issues		The notification of all data exchange entities, the need for data bridges and filters, contingency plans if no data are received from an external source, validation process for incoming external data, contingency plans for invalid data.	In Process
		Identify interdependencies		Identify the internal and external dependency links between enterprise core business areas, processes, and information systems.	Complete
			Identify Year 2000 vulnerable systems and processes	Identify and assess Year 2000 vulnerable systems and processes including those outside the SVP management area, i.e., telephone and network switching equipment, and building infrastructure systems.	Complete
			Transmission Agencies (Grid)		Complete
			Energy Suppliers		Complete
			Energy Trading		Complete
			Customers		Complete
			Vendor Services		In Process
		Gather and evaluate information re:			In Process
			interactions		On Going
			suppliers		On Going
			business partners		On Going
			customers		On Going
			product compliance		Complete
		Liaison			
			Establish Liaison Required	Identify with whom liaison is required - internal and external.	On Going
			Contact Customers	Establish readiness liaison with Customers.	On Going
			Contact Suppliers (of Materials and Services)	Establish readiness liaison with Suppliers.	On Going
			Review the Effects on any Internal Documentation	Does any of the information obtained affect internal documentation?	On Going
			Review the Effects on any Internal Procedures	Does any of the information obtained affect Internal Procedures?.	On Going
Renovation				The renovation–repair, replacement, or retirement–phase involves making and documenting changes to systems and equipment.	
	Determine what equipment needs to be retired,			All items identified in Assessment.	Complete
	Order extra supplies				In Process
	Repair or convert selected applications, databases, archives, systems, system			In converting application systems, consider changes in operating systems, compilers, utilities, domain-specific program products, and commercial database management systems.	In Process

Guidelines - Tasks Status

FXHIBIT C

SVP ᐧ ⎯AR 2000 PROJECT GUIDELINES

8/10/99

	Replace selected applications, platforms, systems, system components, equipment, etc.			Ensure that replacement products are Year 2000 compliant, including their ability to properly handle the leap year adjustments. Direct contract specialist and legal staff to review contracts and warranties.	**In Process**
		Order equipment replacements			**In Process**
		Install replacements			**In Process**
	Retire selected applications, platforms, systems, system components, equipment, etc.			Also retire replaced applications, equipment, etc., upon the successful completion of acceptance testing of replacement.	**In Process**
	Develop data bridges and filters			Ensure that all internal data sources meet the Year 2000 date standards of the converted or replaced systems. Develop bridges or filters to convert non-conforming data.	**In Process**
	Document code and system changes			Implement and use configuration management procedures to ensure that all changes to information systems and their components are properly documented and managed.	**In Process**
	Communicate changes to all internal and external users			Communicate changes to systems and components, and specifically all changes to date formats for data exchanged with other systems or external organizations. Document changes through the configuration management process.	**In Process**
	Share information among Year 2000 projects and			Disseminate via as Internet and intranet sites, meetings, memos, etc.	**On Going**
Validation				The length of the validation and test phase and its cost are driven by the complexity inherent in the Year 2000 problem. SVP will not only test Year 2000 compliance of individual applications, systems and equipment but also the complex interactions between converted or replaced computer platforms, operating systems, utilities, applications, databases, and interfaces. All repaired or replaced system components must be thoroughly validated and tested to (1) uncover errors introduced during the renovation phase, (2) validate Year 2000 readiness, and (3) verify operational readiness. The testing should take place in as realistic an environment as possible.	
	Develop validation strategies and testing plans for				
	Identify and acquire Year 2000 tools			SVP will, if necessary identify and acquire Year 2000 tools to facilitate the conversion and testing processes.	**Complete**
	Prepare Test Plan			Define, collect, and use to manage the testing and validation process.	**In Process**
		Prepare Test Data		Set-up adequate test data.	**Complete**
				Determine what devices use date information for. Do the devices perform load control or other switching functions based on date information.	**Complete**
				Ensure compliance statements have been received for critical devices before proceeding with testing.	**Complete**
				Bench-test sample devices where practical.	**On Going**
		Schedule unit, integration, and system tests		Schedule unit, integration, and system tests following the repairs on individual applications, software modules or equipment. Coordinate scheduling to ensure that all components-including data bridges or filters--are compatible.	**On Going**
		Perform System Tests		Run program/system tests.	**In Process**
			Perform unit, integration, and system testing	Using a phased approach, perform unit, integration, and system testing. Use selected testing techniques to ensure that the converted or replaced systems and accompanying components are functionally correct and Year 2000 ready.	**In Process**
			Test renovations		
			Test replacements	Suspect devices with reported but unconfirmed operational problems should be scheduled for replacement with new Year 2000-compliant devices. In cases where very few devices are deployed in the field, it may be most cost-effective to replace rather than to fix.	**In Process**

EXHIBIT C

SVP \ ⊏AR 2000 PROJECT GUIDELINES

8/10/99

		Develop a strategy for managing the testing of contractor-converted systems	The contract conversion must be closely managed to ensure that the contractor follows the SVP's Year 2000 conversion standards. In addition, SVP must ensure that the contractor-converted systems are adequately tested.	**In Process**
		For each converted, repaired, or replaced application or system component, or equipment develop and document test and	Establish a compliance validation process. Note: Most suppliers of COTS software do not disclose their source code or the internal logic of their products; therefore, testing should be complemented by a careful review of warranties and/or guarantees.	**In Process**
		Amend Progs/Systems where required	Amend where problems have arisen resulting from tests	
		Finalize Integrated System Test.	Re-run until fault free.	
	Initiate acceptance testing		Acceptance testing is the final stage of the multiphase testing and validation process. During this phase, the entire information system--including data interfaces--is tested with operational data. In general, acceptance testing should be done on the Year 2000 test facility with duplicate database to avoid risk to the production systems and the potential contamination of data.	**In Process**
Implementation			Implementation of Year 2000 compliant systems and their components require extensive integration and acceptance testing to ensure that all converted or replaced system components perform adequately in a heterogeneous operating environment. Once converted or replaced simultaneously, SVP may be expected to operate in a heterogeneous computing environment comprised of a mix of Year 2000 ready and non-ready applications and applications and components into the SVP's production environment must be carefully coordinated to account for system interdependencies. Parallel processing--where the old and the converted systems are run concurrently--may be needed to reduce risk.	**In Process**
	Develop implementation schedule			**On Going**
	Define transition environment and procedures		Some key components of SVP systems--Year 2000 ready databases, operating systems, utilities, and other COTS products--may not be available until late 1998 or early 1999. Second, external data suppliers may not plan to complete their conversion and testing until 1999. Third, the testing, validation, and correction processes may take much of 1999. Fourth, replacement systems may not be ready for testing until late 1999. As a result, SVP may be forced to operate--at least for a time--parallel systems and databases.	**In Process**
	Implement overall Project Strategy			**On Going**
		Resolve data exchange issues and interagency concerns	All outside data exchange entities are notified, data bridges and filters are ready to handle non-conforming data, contingency plans and procedures are in place if data are not received from an external source, contingency plans and procedures are in place if invalid data are received from an external source, the validation process is in place for incoming external data. All data issues and interagency concerns should be resolved prior to acceptance testing and implementation. Bridges and filters should be in place to handle non-confirming data received from external sources, and contingency plans and procedures should be in place to handle no data or bad situations.	**In Process**
		Implement converted and replaced systems	Reintegrate the converted and replaced systems and related databases into the production environment.	**In Process**
		Deal with database and archive conversion	Because the conversion of large database from 2-digit to 4-digit year fields is a time consuming effort, SVP may consider off-site conversion alternatives if necessary.	**In Process**
	Live-Run The System Phase			
		Load New Programs	Load and run Live System.	**In Process**
		Close the Current System	Close-down and transfer data to new system.	

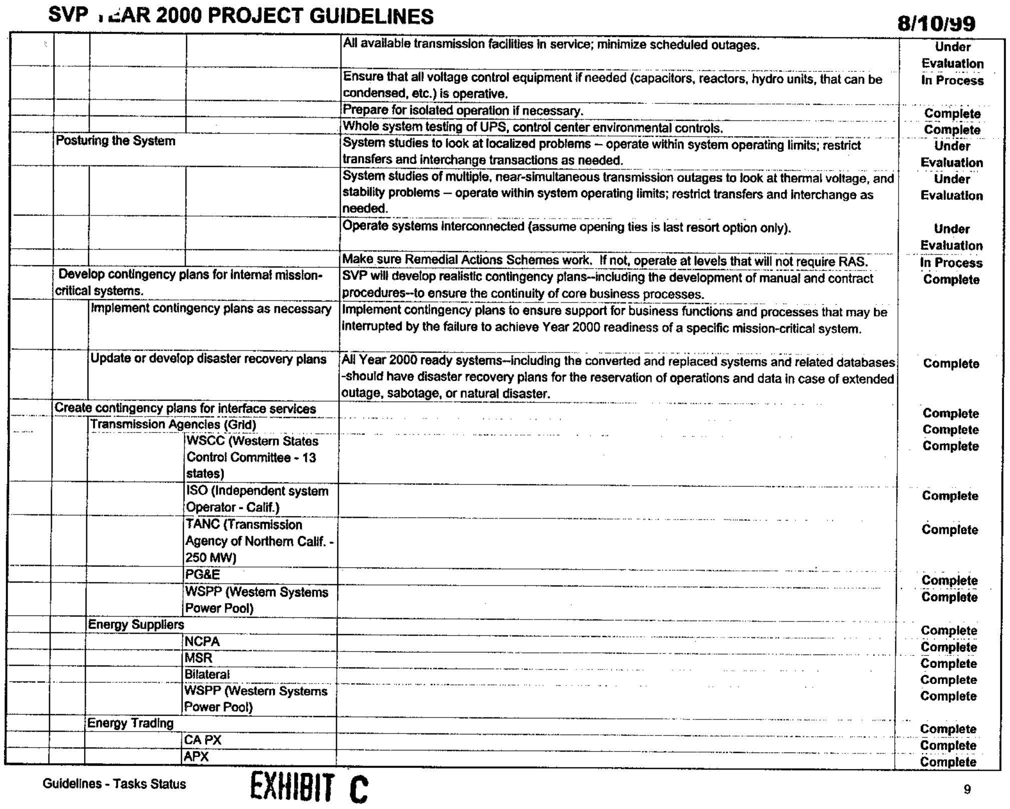
EXHIBIT C

SVP . _AR 2000 PROJECT GUIDELINES

8/10/99

		Complete acceptance testing	In general, formal testing uncovers about 80-90 percent of software errors, with the remaining 10-20 percent of errors discovered during operations. Acceptance testing should be completed no later than Fall of 1999, to allow sufficient time for the correction of software errors discovered following implementation.	
	Complete Systems Audit		Formalize the internal/external audit requirements.	
	Approve System		Document the Approved system.	
Risk Management/Contingency Planning				
	Staffing		Key technical support staff available on-site at critical stations and control centers; staff remotely operated plants.	**Complete**
			Critical IT staff available to recover EMS/SCADA	**Complete**
			Maintain sufficient operating personnel at control center. This may include additional dispatchers, plant operators and switching personnel.	**Complete**
			Man major generation and transmission facilities.	**Complete**
	Operating Procedures		Load shedding plan ready.	**Complete**
			Black start capability and restoration plans ready.	**Complete**
			Control areas prepared to go on constant frequency control under islanding conditions; generating units prepared to operate on frequency control in the event of islanding.	**Complete**
			Control center contingency recovery plan.	**Complete**
			Testing of UPS, control center environmental controls.	**Complete**
			Identify manual monitoring and operating procedures, train personnel, conduct drills.	**Complete**
	Market		Coordinate with market and IPPs for generation availability.	**In Process**
			Communicate transmission mitigation strategy to the market (including possible reduction in transfers).	**In Process**
	Generation		More generation on-line (units which are Y2k ready); minimize scheduled outages; evaluate minimum generation considerations.	**Under Evaluation**
			Strategic location and amount of operating reserves.	**Under Evaluation**
			Units prepared to operate on frequency control in the event of islanding.	**Under Evaluation**
			Whole unit Y2k tests of critical units.	**Under Evaluation**
	Communication		Radio communications available as backup to primary voice communications to manual monitoring and control; backup up radio systems tested.	**Complete**
			Develop back up communications plan for SVP and control areas. Back up plan should include real time marketing personnel as schedule adjustments may be required.	**Complete**
			Establish an advanced warning system of monitoring electrical systems. The purpose of this system would be to provide moment to moment assessments of potential risks during the 1999-2000 transition.	**Complete**
			Backup radio systems tested and available.	**Complete**
			Identify, maintain and test older data systems that may be used during Y2k, including power line carrier.	**In Process**
			Procedures and drills for operation without data and primary voice communication systems	**Complete**
			Plan, test, and train backup voice communications.	**In Process**
	Facilities		Test backup power supplies for facilities.	**On Going**

EXHIBIT C



SVP ı ≤AR 2000 PROJECT GUIDELINES

8/10/99

				All available transmission facilities in service; minimize scheduled outages.	Under Evaluation
				Ensure that all voltage control equipment if needed (capacitors, reactors, hydro units, that can be condensed, etc.) is operative.	In Process
				Prepare for isolated operation if necessary.	Complete
				Whole system testing of UPS, control center environmental controls.	Complete
	Posturing the System			System studies to look at localized problems – operate within system operating limits; restrict transfers and interchange transactions as needed.	Under Evaluation
				System studies of multiple, near-simultaneous transmission outages to look at thermal voltage, and stability problems – operate within system operating limits; restrict transfers and interchange as needed.	Under Evaluation
				Operate systems interconnected (assume opening ties is last resort option only).	Under Evaluation
				Make sure Remedial Actions Schemes work. If not, operate at levels that will not require RAS.	In Process
	Develop contingency plans for internal mission-critical systems.			SVP will develop realistic contingency plans--including the development of manual and contract procedures--to ensure the continuity of core business processes.	Complete
		Implement contingency plans as necessary		Implement contingency plans to ensure support for business functions and processes that may be interrupted by the failure to achieve Year 2000 readiness of a specific mission-critical system.	
		Update or develop disaster recovery plans		All Year 2000 ready systems--including the converted and replaced systems and related databases -should have disaster recovery plans for the reservation of operations and data in case of extended outage, sabotage, or natural disaster.	Complete
	Create contingency plans for interface services				Complete
		Transmission Agencies (Grid)			Complete
			WSCC (Western States Control Committee - 13 states)		Complete
			ISO (Independent system Operator - Calif.)		Complete
			TANC (Transmission Agency of Northern Calif. - 250 MW)		Complete
			PG&E		Complete
			WSPP (Western Systems Power Pool)		Complete
		Energy Suppliers			Complete
			NCPA		Complete
			MSR		Complete
			Bilateral		Complete
			WSPP (Western Systems Power Pool)		Complete
		Energy Trading			Complete
			CA PX		Complete
			APX		Complete

Guidelines - Tasks Status

EXHIBIT C

9

SVP YEAR 2000 PROJECT GUIDELINES

8/10/99

			COB		Complete
		Customers			Complete
		Vendors			Complete

EXHIBIT C

Y2K

Notes:

What is the Y2K Problem?

The Y2K technology problem, also called the "millennium bug", is something we have inherited from the early days of computers. Back then, computer memory was scarce and expensive, so programmers used a 2-digit entry to designate each year instead of a 4-digit entry. For example, 1999 was entered as 99.

Unfortunately, the 2-digit date format cannot process dates in two different centuries. So when the year 2000 arrives, systems that have the 2-digit year codes may interpret the year "00" to be "1900". These systems simply cannot tell the difference between the years 2000 and 1900 unless they have been fixed ahead of time.

However, 1/1/2000 is not the only critical date! In fact, some experts believe that as few as 8% of Y2K problems will occur on 1/1/2000; the rest will occur at another time.

Who Could Be Affected?

Any person using or communicating with a computer or computer-driven product or system could be affected. Remember that the systems that could be affected are not just the actual "computers" or computer software. Any equipment with "embedded" computer chips could be affected.

What Infrastructure Systems Could Be Affected?

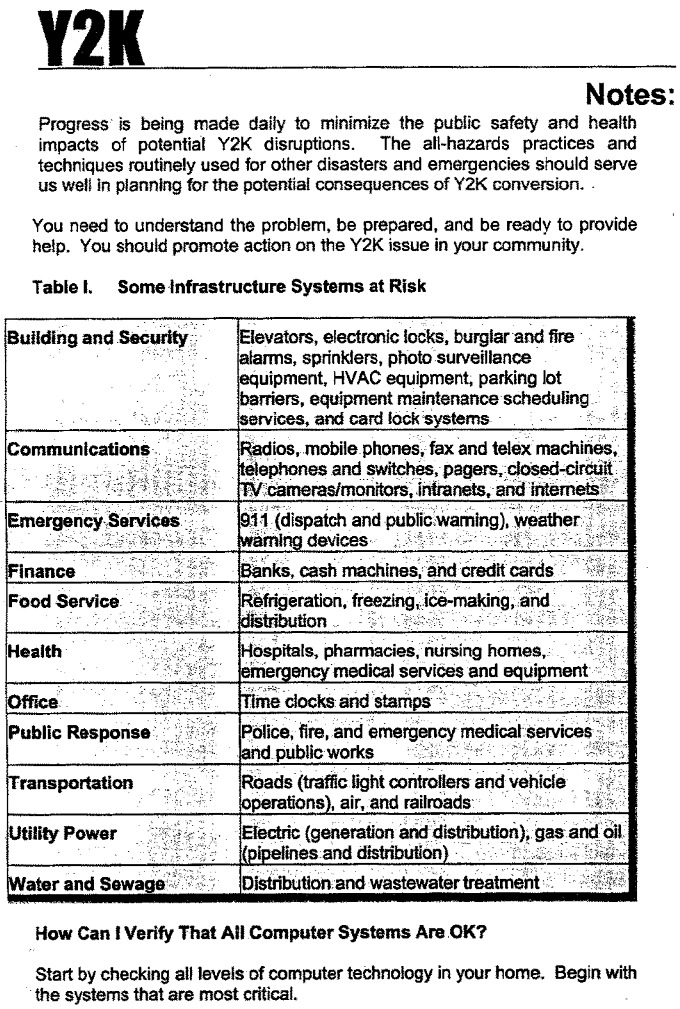
Progress is being made in ensuring that City systems are Y2K compliant. Still, failures could occur in some systems. Table I shows some of the systems and associated devices that could be affected.

The interconnectedness of many of these systems creates part of the risk associated with the Year 2000.

Why Should I Be Concerned About the Year 2000 Problem?

The computerized systems that may fail as a result of the bug could have an impact on our community – the same kind of impact as a natural or man-made disaster. For example, if electrical systems fail, people may need shelter, food, water, information, transportation assistance, financial help, etc.

EXHIBIT D



Y2K

Notes:

Progress is being made daily to minimize the public safety and health impacts of potential Y2K disruptions. The all-hazards practices and techniques routinely used for other disasters and emergencies should serve us well in planning for the potential consequences of Y2K conversion.

You need to understand the problem, be prepared, and be ready to provide help. You should promote action on the Y2K issue in your community.

Table I. Some Infrastructure Systems at Risk

Building and Security	Elevators, electronic locks, burglar and fire alarms, sprinklers, photo surveillance equipment, HVAC equipment, parking lot barriers, equipment maintenance scheduling services, and card lock systems
Communications	Radios, mobile phones, fax and telex machines, telephones and switches, pagers, closed-circuit TV cameras/monitors, intranets, and internets
Emergency Services	911 (dispatch and public warning), weather warning devices
Finance	Banks, cash machines, and credit cards
Food Service	Refrigeration, freezing, ice-making, and distribution
Health	Hospitals, pharmacies, nursing homes, emergency medical services and equipment
Office	Time clocks and stamps
Public Response	Police, fire, and emergency medical services and public works
Transportation	Roads (traffic light controllers and vehicle operations), air, and railroads
Utility Power	Electric (generation and distribution), gas and oil (pipelines and distribution)
Water and Sewage	Distribution and wastewater treatment

How Can I Verify That All Computer Systems Are OK?

Start by checking all levels of computer technology in your home. Begin with the systems that are most critical.

EXHIBIT D

Y2K

Notes:

How Can I Tell If I Have an Embedded Chip Product?

Check to see if it:

- Has an LED (light-emitting diode) maintenance or operations panel with menu options
- Stores data for further use
- Has an internal clock
- Has controls for changing functions on the basis of times or dates
- Communicates with the user either visually or with sound
- Displays a time/date

How Do I Develop an All Hazards Contingency Plan?

An All-Hazards Plan is a plan that will work for all known hazards such as an earthquake or flood. Y2K comes under the classification of a technical hazard. All-Hazards planning has four basic steps:

□ Identify the problem areas
□ Develop the plan
□ Test it
□ Implement the plan

These steps will help you deal with potential Y2K problems and help you find a stable, workable solution.

When Should I Plan?

Start now! Just as when you develop plans for other hazards, you must allow enough time to test your plan before you need to activate it. We can't tell you which time frames to use, because there are so many variables. If you are just beginning, here are some possible time frames for communities in the planning process:

Identify the problem areas	June – July 1999
Develop the plan	July – August 1999
Test the plan	September – October 1999
Revise the plan as needed	Up to November 1999
Implement the plan	December 1999 – Jan. 2000

EXHIBIT D

Notes:

How Can I Help Others to Prepare?

To relieve anxieties and help prepare for Y2K, you should tell others that the government at all levels, as well as business and industry, are working together to solve the problem and ensure that public health and safety services won't be disrupted when the new millennium starts.

Encourage everyone to get more involved in all-hazards emergency planning, and understand the emergency procedures.

Everyone should prepare for Y2K disruptions in the same way one prepares for other problems, such as winter storms or earthquakes.

What Can I Do About These Devices?

Conduct an internal inventory to identify all items that may contain chip technology and all services that depend on them. Then try to check whether each product is Y2K compliant.

You should request letters certifying Y2K compliance from all of the applicable vendors. Be sure they describe the methods they used to determine compliance. If a vendor/supplier says its product is not compliant, develop a contingency plan to either replace the product or to deal with its failure.

When Will the Problem Strike?

Most of the publicity about Y2K points to problems on January 1, 2000. But that is not the only critical date. Some experts predict a string of malfunctions throughout 1999 and 2000, rather than a single calamity. Why is this the case? Because programmers enter dates differently in different systems and products. Table 4 lists some of the dates that could cause problems and explains why.

How to Organize A Neighborhood or Group

While it is important to prepare for Y2K as an individual and as a household, the best preparedness is having prepared neighbors. By working together, we can achieve far more than we could alone. By building trusting relationships now, we will be better able to rely on each

EXHIBIT D

Notes:

other if there are challenges. By encouraging our neighbors to prepare, we ensure our own safety and well being, and the security and resilience of our community.

There are many ways to organize your neighborhood, block, apartment building, congregation or other group. Effective methods include calling a meeting, putting up flyers, inviting people to come together to discuss Y2K and sharing the information in this article. When organizing a large neighborhood, it may be useful to ask people to volunteer to be block captains over smaller areas. When calling the first meeting, it may be useful to invite an outside speaker to give a presentation on Y2K. The Santa Clara Fire Department can help. They can be contacted at (408) 984-3062. The following is a list of possible approaches to community organizing. Feel free to adapt this to fit your particular needs, interests and abilities:

- Encourage and assist each household in conducting their own household preparedness.
- Get together and buy items in bulk in order to get a better price (everything from food to flashlights may be available wholesale if you buy in large quantities).
- Buy large items such as a camp stove or solar generator as a group and make plans for shared use.
- Perform a door-to-door "special needs" assessment to determine who might need extra help if there are disruptions; and come up with a way to provide such help (such as a buddy system).
- Perform a skills/resources assessment so the community will know in advance where to find medical help, special tools, and other things which might be useful.
- Come up with a communication/information system. This could include a shared ham (amateur) radio, a system of walkie-talkies, and a bulletin board posted in a public place in your area (the person with the radio or information could post it on the bulletin board for everyone to see).
- Have the group sign up for CPR and First Aid training. The American Red Cross offers this training and they can be contacted at (408) 577-2178.
- Sign up together to take Santa Clara Fire Department's HEAT (Home Emergency Assistance Teams) Training Program. This six part program is designed to help the citizens of Santa Clara be self sufficient after a major disaster by developing multi-functional teams that are cross trained

EXHIBIT D

in basic emergency skills. Call the Santa Clara Fire Department at (408) 984-3239 for more information and/or to enroll.

Table 3. Important Dates for Y2K

December 31, 1999 – January 1, 2000	Last day of 1999,first day of 2000
September 9, 1999	May be mistaken for“end of file” code
February 29, 2000 – March 1, 2000	Uncommon leap year
August 22, 1999	Rollover date for GPS systems

Resources for Helping the Public Prepare for Y2K

The President's Council on Year 2000 Conversion has expanded its web site http://www.y2k.gov/, creating a separate area devoted to consumer issues and the Y2K problem. The information in this part of the site is similar to that described in the next paragraph, but users can also link directly to the agencies, companies, and industry groups that are the primary sources for much of the existing information on Y2K efforts.

Individuals can also call the number **1-888-USA-4-Y2K** to get information about power, telephones, banking, government programs, household products, and other common topics. This information comes from primary sources – government agencies, companies, or industry groups. Information specialists, supported by researchers, are available to provide additional information to callers. Pre-recorded information is available seven days a week, 24 hours a day. Information specialists staff the line from 9 AM to 8 PM (EST), Monday through Friday. The service also has “FAX-back” capability.

The Federal Trade Commission (FTC) also has Y2K publications for consumers on consumer electronic products, home office equipment, and personal finances. These publications are available on-line at http://www.ftc.gov and through FTC's Consumer Response Center at 202-FTC-HELP. It also has a Business Fact Sheet urging businesses to disclose the Y2K status of their products to their consumers.

Assistance is also available for small businesses and service providers. The Small Business Administration (SBA), the National Institute for Standards and Technology's Manufacturing Extension Program, and the

EXHIBIT D

Y2K

Notes:

President's Council on Year 2000 Conversion have compiled many Y2K tools for small businesses and critical service providers. Information about these tools can be found on their web sites: http://www.sba.gov/, http://www.mep.nist.gov/, and http://www.Y2K.gov/. Small- and medium-sized businesses can also call 1-800-U-ASK-SBA for information on Y2k.

In addition, the State of California has web pages devoted to the Y2K problem. These pages provide information, additional planning guidance, tools and procedures, and links to other Y2K-related web sites.

The American Red Cross has the following documents that are available to all:

- ***Your Family Disaster Plan –***
  How to prepare for any type of disaster
- ***Your Family Disaster Supplies Kit –***
  A checklist of emergency supplies
- ***Emergency Preparedness Checklist –***
  An action checklist on disaster preparedness
- ***Helping Children Cope with Disaster –***
  How to help children deal with the stress of disaster

All four documents are available in Spanish. You can find these helpful documents and others on-line. Also, check the American Red Cross web site for specific information about preparing for Y2K. These preparations should include:

- Checking with manufacturers of any essential computer-controlled equipment in the home
- Preparing supply kits for family disasters
- Checking home smoke alarms and buying extra batteries
- Keeping a battery-operated radio or television available to be able to receive emergency television

The easiest and quickest way to obtain a wide range of current Y2K information is by examining the many Internet web sites dedicated to this issue. By looking at the World Wide Web, you can discover the nature and magnitude of Y2K problems, see what others are doing to solve these problems, and obtain contingency planning information from organizations and governments.

EXHIBIT D

Y2K

Notes:

The following list of representative web sites can help you get started. This list is a pathway to web sites that contain specific information and can lead you to other sources of useful information. The addresses of these sites have been reduced to the minimum number of characters needed to get you to the site. Once there, you can follow links to obtain more detailed information within and outside of the site.

Selected Web Site Listings

http://www.y2k.gov/
The President's Council on Year 2000 Conversion – provides status reports and information for consumers on how the Y2K problem may, or may not, affect their daily lives. For links to many sites dedicated to fixing systems, select "Text" or "Graphics", select "Becoming Y2K Compliant", then select "Tool Kit: Understanding your Organization's Y2K Challenge".

http://www.fema.gov/
FEMA Year 2000 Issues – FEMA provides information and web links to additional information on emergency service, and emergency response, preparedness and contingency planning.

http://www.usfa.fema.gov/
The National Fire Data Center – answers some frequently asked questions (FAQs) and lists Y2K web sites of importance.

http://www.nstl.com/
The National Software Testing Lab – provides shareware to test computers for Y2K compliance.

http://www.redcross.org/
The American Red Cross – answers some FAQs and provides individuals with a checklist of actions to follow for preparedness.

http://www.senate.gov/~y2k/
The U.S. Senate Special Committee on the Year 2000 Technology Problem – provides links to governmental agencies.

http://www.year2000.com/
Year 2000 Information Center – provides a forum for exchanging information and possible solutions to Y2K problems.

EXHIBIT D

San Jose Mercury News Survey Response

1. What are your top 10 mission critical systems?

Of the systems that are considered mission critical to Silicon Valley Power's successful operation, none would block the utility's ability to supply power to its customers. The systems that are considered mission critical to Silicon Valley Power include systems for power trading, for electronic metering of customers power use, for power distribution monitoring, and other systems that enable or enhance our business processes. All of these systems have either been replaced or remediated to ready them for operation into the year 2000. Again none of these systems would stop the supply of power to Silicon Valley Power customers.

2. Have you done an inventory of all of your computer equipment to find out what might need year 2000 remediation? When did you start? Have you finished yet?

Last year Silicon Valley Power conducted an internal inventory and assessment of all computer equipment and systems and contracted with a Year 2000 consulting firm for an inventory and assessment of all embedded systems. These inventories and assessments were completed in 1998.

2. What percentage of your critical systems are now Y2K compliant?

All of Silicon Valley Power's critical systems are Year 2000 ready, however we will continue to monitor, assess, and all of our systems for potential Year 2000 problems. We are also continuing to upgrade and replace non-critical equipment and systems to minimize any impact from any unforeseen problem.

4. By Jan. 1, 2000, will all critical systems be fully Y2K compliant?

See response to question two.

5. What is your target date this year for 100 percent Y2K compliance for critical systems?

See response to question two.

6. Do you have a formal, written contingency plan to serve customers and carry on operations in the event of Y2K disruptions?

For over 100 years of operation as an electric utility, Silicon Valley Power, has and will continue to be prepared to provide uninterrupted service to our customers. We have formal written emergency plans to maximize this ability in the event of outside disruptions such as floods and earthquakes. These

EXHIBIT E

emergency plans serve as the basis for enhanced and additional contingency plans specific to Year 2000. We will continue to develop and refine our existing plans as long as there are potential Year 2000 problems, and believe that these activities will provide us with improved plans for other potential future emergencies.

7. What have you run tests on for Y2K compliance? What were the results?

See response to question two.

8. What work has been done in the emergency services area to train transition teams, create backup communication options, address public concerns, ready emergency vehicles, call boxes and 911, and generally prepare for problem responses?

Silicon Valley Power's Year 2000 project team has and continues to work will all Silicon Valley Power divisions and staff on developing plans that addresses each of these issues and many others. With the support of executive management we have prepared backup communication options, additional training needs, a variety of communication vehicles with our customer, along with other activities to prepare ourselves, our staff, and our customers for potential Year 2000 problem responses.

9. Have you had to change security systems at public buildings?

All of the buildings and facilities used by Silicon Valley Power will be accessible through the Year 2000 without the necessity of any security system changes.

10. What are your plans to collect taxes or other fees, or to disburse checks and pay bills in the event of a computer failure caused by the millennium bug?

The City of Santa Clara has the primary responsibility for these activities on the behalf of Silicon Valley Power and this question would be best addressed by the general City administration.

11. What critical outside suppliers are you dependent on? Have you surveyed providers of water, waste disposal, sewage treatment, power, phone services and other critical areas?

Silicon Valley Power contracts for the supply of power from many sources including a variety of joint power agencies of which we are a member. Most of the power supplied to Silicon Valley Power customers is generated outside of the City at facilities owned by a variety of agencies including the City and transmitted to the City through lines owned by the Pacific Gas and Electric Company. These agencies have indicated that their systems will be ready for the Year 2000 roll over. However, we will continue to work with Pacific Gas and Electric, and other energy providers either individually or through other agencies such as the

EXHIBIT E

California Independent Systems Operators and the Western States Coordinating Council.

12. Who is in charge of Y2K preparations in your agency? How senior is that person in your organization?

Silicon Valley Power has a Year 2000 Project Team consisting of members from each division of the utility. The Team reports to the Executive management of Silicon Valley Power, which includes the Director, Assistant Directors, and some Division Managers. The Team is lead by a Division Manager, who is part of this management team.

13. What are your staffing plans for the end of 1999 and the beginning of 2000?

Silicon Valley Power will have specific personnel on site during the end of the year roll over who will be best able to handle any potential problems. We are also in the process of developing additional staffing plans that would include more remote eventualities and backup personnel.

14. What costs have you incurred? Are you making additional appropriations? Where are your largest expenses occurring?

Many of the activities that will minimize Silicon Valley Power Year 2000 vulnerabilities were undertaken for reasons that were unrelated to the Year 2000. Thus the costs of them have not been directly attributed to Year 2000 preparations. Silicon Valley Power has however appropriated in the 1999/2000 budget a capital project for Year 2000 related equipment replacement. Our largest expenses directly attributable to Year 2000 activities have been for third party inventory and assessment services and Silicon Valley Power staff time.

15. What have you done to inform residents and customers of your progress in fixing Y2K problems? Have you posted your agency's progress on your Web site? What is your Web site address?

Silicon Valley Power has joined with other City departments on activities to provide Year 2000 information to City residents, including mailings, newspaper articles, and prcsentations to Council that are broadcast over the City government cable channel. For our commercial and industrial customers, Silicon Valley Power has conducted a series of meetings that will continue into the new year to provide them with ongoing reports and siatus of our Year 2000 preparation activities.

16. Have you encouraged citizens to do anything to prepare for Y2K?

The City of Santa Clara has the primary responsibility for these activities on the behalf of Silicon Valley Power and this question would be best addressed by the general City administration.

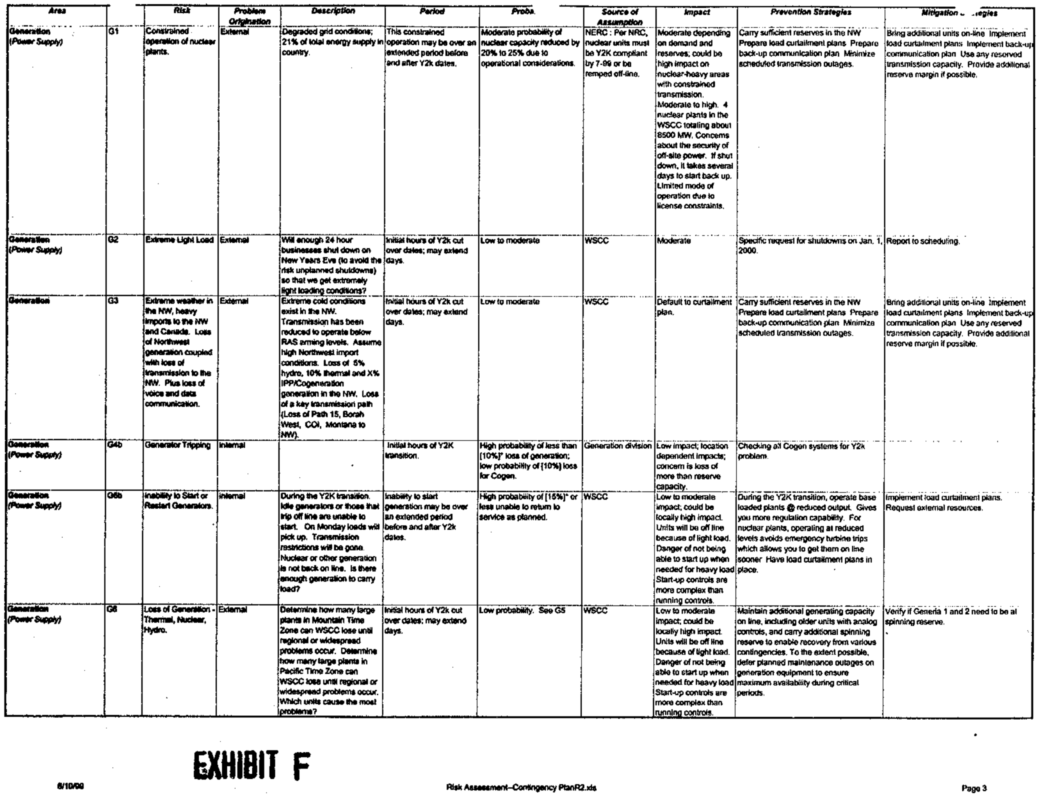
EXHIBIT E

Area		Risk	Problem Origination	Description	Period	Probab.	Source of Assumption	Impact	Prevention Strategies	Mitigation S..ategies
Communications *(Comm.)*	C1	Voice / Land lines	External	Loss of internal and external communication lines.	Initial hours of Y2k cut over dates; may extend days.	Low to moderate	NERC/ WSCC	High impact for coordinating operations.	Work with telecommunications providers to ensure availability of critical communications facilities. Develop a back-up communication plan. Monitor Y2k -related developments as far to the east as possible on December 31, 1999 (perhaps as far as the international dateline) to gain early warning of problems that may be occurring. Hard wire phone lines between EOC and Operations	Use radio, pagers, cell phones, couriers, and/or face-to-face communications.
Communications *(Cash Flow/Trading)*	C2	Automatic funds Transfer	External	Inability to transfer funds	Initial hours of Y2k cut over dates; may extend days.	Low to moderate	WSCC	Moderate to High	Work with finance and banks to ensure availability of critical tranfer abilities. Develop a back-up communication plan. Prepare backup plan with critical customers for other forms of payment.	Cash on hand- determined by anticipated staffing
Communications *(Data Mgmt.)*	C3a	Data/Telemetry Messaging (WON) Other data links ICCP links analog lease lines.	Internal / External	Loss of company-owned data communication; includes real-time and non real-time data. Loss of the WON, EHV Data Pool, ICCP links, etc.	Initial hours of Y2k cut over dates; may extend days.	Moderate to high probability of loss of portion of company owned data communications due to high degree of networking and interdependence.	Trading Manager	Medium impact for partial loss of data communications. High impacts on protection, control, and monitoring.	Identify equipment, circuits, path connectivity. Determine risk. Propose/develop contingency communications plan.	Implement Communication Plan to acquire sufficient information to operate the system.
Communications *(Metering)*	C3b	Loss of Data from smart/advanced meters (MV90)	Internal / External	Unable to collect data or data is incorrect.	Initial hours of Y2k cut over dates; may extend days.	Low	Metering	Moderate impact, low profile data	Identify equipment, circuits, path connectivity. Determine risk. Propose/develop contingency communications plan.	Implement Communication Plan to acquire sufficient information to operate the system.
Communications *(SCADA/Operations)*	C4	SCADA: Partial loss of capabilities (including EMS overload during burst of high activity).	Internal/ External	No communication with RTUs.	Initial hours of Y2k cut over dates; may extend days.	Moderate probability of loss of some EMS/SCADA functions; low probability of loss of some RTUs.	SVP Project Team	High impact due to loss of system data for critical functions; Impact of data is high. We would be blind. Critical to communications and load curtailment	Replace system	Manual reads and control function.
Communications *(SCADA/Operations)*	C5	Global Position Systems (GPS).	External	Incorrext time records.	Initial hours of Y2k cut over dates; may extend days.	Low to moderate	WSCC	Low to moderate		Manual reads and control function
Communications *(SCADA/Operations)*	C6	Multi-loop control and monitoring - DCS, SCADA, Telemetry.	Internal	Monitoring loss of Daytel.	Initial hours of Y2k cut over dates; may extend days.	Moderate	WSCC	Scheduling would be blind. Lack of data for scheduling.	Upgrade clock cards and drivers.	Back up lap top reads at KRS and SRS.
Communications *(Comm.)*	C7	Pagers	External	Missed and erroneous pages.	Initial hours of Y2k cut over dates; may extend days.	Low to moderate	WSCC	Marketing-moderate Systems-Low	Check with vendors	Use cell phones. Use periodic call-ins or face-to-face communications.
Communications *(Comm.)*	C8	Radio	Internal	Reduce Communications	Initial hours of Y2k cut over dates; may extend days.	Low to moderate	WSCC	Operations	Check with vendors; test tach lines.	Use cell phones. Use satellite phones.
Communications *(Comm.)*	C9b	Cell Phones	External	Reduced ability to communicate.	Initial hours of Y2k cut over dates; may extend days.	Low to moderate	Communicate	Operations, Cust. Serv.	Check with vendors	Use radio, satellite radios, runners.
Communications OPEN	C10	Uncontrolled cascading events result in Islanding. Plus loss of voice and data communication.	Compound	Loss of power	Initial hours of Y2k cut over dates; may extend days.	Low probability	WSCC	High	Have black start procedures ready and dispatchers trained. Prepare back-up communication plan. Have internal generation on-line.	Implement black start procedures. Implement back-up communication plans.
Energy Distribution *(Energy Dist.)*	D1	Loss of distribution systems.	Internal	Partial to total black-out.	Initial hours of Y2k cut over dates; may extend days and weeks.	Low to moderate	WSCC	High impact on locally affected customers.	Prepare for black start capabilities. Prioritize where any flow could or should be sent, i.e. health and safety concerns 1st.	Will have SVP crews on call; including three operators, one manager and senior manager. (May change)
Energy Distribution *(Power Supply)*	D2	Loss of transmission to City.	External	Total black-out.	Initial hours of Y2k cut over dates; may extend days and weeks.	Low	SVP Project Team	High impact on locally affected customers.	Prepare for black start capabilities. Prioritize where any flow could or should be sent, i.e. health and safety concerns 1st.	If island or total blackout; Use portable generators. Where to direct flow of internal generation, to which customers?
Equipment *(Facilities)*	EQ1	Backup lighting and generators.	Internal	Loss of interal generator	Initial hours of Y2k cut over dates; may extend days.	Low	WSCC	Low to moderate if external power is available	Testing equipment	Portable generators
Embedded Systems *(Energy Dist.)*	ES1	Automatic Control Scheme Failures (SVCs, Substation Capacitor Banks, etc.).	Internal	Run on time clocks	Will trip, but no outage.	Low probability; most banks electro mechanical	SVP Project Team	Low impact on locally affected customers.	Analyze, fix by removing them from automatic control, or replace, and test . Staff critical areas such as substations and plants. **Needs to assess (?) at leap year.**	Have personnel ready to manually operate equipment if necessary.

EXHIBIT F

Area		*Risk*	*Problem Origination*	*Description*	*Period*	*Probab.*	*Source of Assumption*	*Impact*	*Prevention Strategies*	*Mitigation . .egies*
Embedded Systems *(Facilities)*	ES2	Environmental monitoring and control systems.	Internal	HVAC loss	Initial hours of Y2k cut over dates; may extend days.	Low probability of loss of some environmental monitoring systems.	WSCC and NERC	Low impact if loss of available generation more than reserves.	Develop and test procedures for operation without energy management systems. Ensure all remedial action schemes are Y2k ready. If not certain, operate at levels that will not require remedial action to take place. Shut down equipment deemed as non-critical if Y2k readiness is not assured. Set clocks back to delay Y2k rollover where desirable and feasible.	Open doors and/or put in heaters
Embedded Systems	ES5a	Programmable Logic Controls (PLCs) and embedded date sensitive controls - transformers, protective relaying, breaker control; field devices - measurement, actuation, recorders; panel-mounted devices, control, display, recording, operations.	Internal	Mis-operation of static controls protective devices	Initial hours of Y2k cut over dates; may extend days.	Low	WSCC and SVP Project Team	Low	Tested. Not date sensitive; basic functions verified.	Reset after leap year.
Embedded Systems *(SCADA/Operations)*	ES7	Remote terminal units (RTUs)	Internal	SOE sync disturbance.	Initial hours of Y2k cut over dates; may extend days.	Low	WSCC	Moderate	Test RTUs in late April. Tested & dependent most in static information.	Have backup staff available for manual operation.
Embedded Systems *(Engery Dist.)*	ES11	Sub-station equipment and system protection (relay) failures resulting in system instability, cascading outage, or facility damage; remedial protection schemes failure.	Internal	SCADA, Basler & Schweitzer relays. Some relays won't recognize leap year in 2000.	Initial hours of Y2k cut over dates; may extend days.	Low probability of system protection tripping facilities; low probability of failure to operate when needed. Manufactures test indicate.	Manufacturer test data. WSCC and SVP Project Team	High impact if failures do occur; results in facility trips possible cascading outages or facility damage.	Have new SCADA system in place and UPS system checked.	Have staff ready to operate manually and monitor. Reset relays for February 29th, 2000.
Embedded Systems *(Engery Dist., Generation, Metering)*	ES12b	Test equipment - used to program, maintain and test control systems.	Internal		Initial hours of Y2k cut over dates; may extend days.	Low			Running NT. Y2k compliant.	Running NT. Y2k compliant.
Embedded Systems *(Cash Flow/Payroll)*	ES13	Time recording systems.	Internal	Loss of automated payroll calculations and check issuance	May extend days.	Low	WSCC	Low	City remediated system	Manual timekeeping and issueing of checks
Embedded Systems *(Facilities)*	ES14a	Traffic Lights	Internal	Traffic lights malfunction.	Initial hours of Y2k cut over dates; may extend days.	Low	WSCC	Low	Test System	Use police to manually direct traffic Use 4-way stop signs.
Embedded Systems *(Transportation)*	ES14b	Vehicles	Internal	Vehicles not operative	Initial hours of Y2k cut over dates; may extend days.	Low	SVP Project Team	Moderate	Assess, Remediate, and Test.	Use other vehicles
Embedded Systems *(Engery Dist.)*	ES15	Voltage control devices misoperate/fail: transformers, capacitor switching; voltage regulators.	Internal	Programmable clocks, voltage control.	Initial hours of Y2k cut over dates; may extend days.	Low probability; tap changers not time dependant, capacitor bank clocks, LTC.	NERC	Moderate impact on power quality.	Assess, Remediate, and Test.	Verify dates after February 29th., 2000.
Facilities *(Fascilities)*	F1	Entry to buildings and areas	Internal	CCA sub-station, Field Admin., Rrading, Operations	Initial hours of Y2k cut over dates; may extend days.	Low probability	SVP Project Team	Low	Assess, Remediate, and Test. Verify if connected to backup generation.	Disable doors and gates.
Facilities *(Fascilities)*	F4	Temperature/ atmospheric controls for computing systems.	Internal	Halon and HVAC malfunction	Initial hours of Y2k cut over dates; may extend days.	Low probability. Halon systems a concern as well as HVAC in computer room.	NERC and WSCC	Moderate impact on functionality if control center evacuation required.	Assess, Remediate, and Test. Verify if connected to backup generation.	Open doors and/or put in heaters

EXHIBIT F

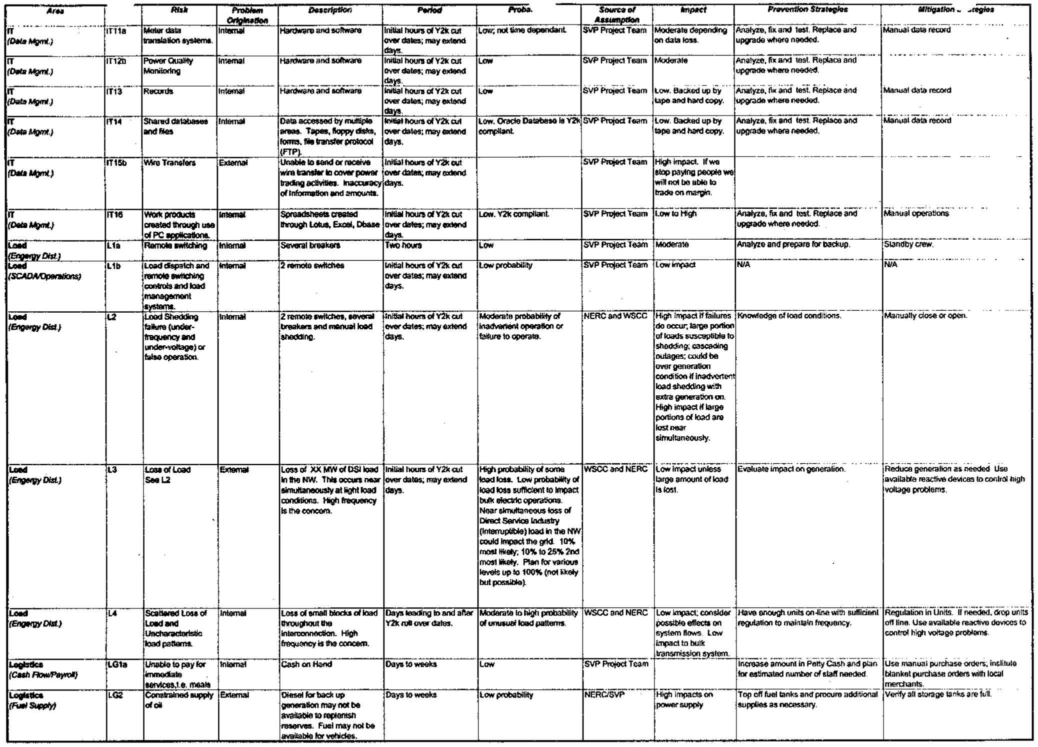


Area		Risk	Problem Origination	Description	Period	Proba.	Source of Assumption	Impact	Prevention Strategies	Mitigation ..egies
Generation (Power Supply)	G1	Constrained operation of nuclear plants.	External	Degraded grid conditions; 21% of total energy supply in country.	This constrained operation may be over an extended period before and after Y2k dates.	Moderate probability of nuclear capacity reduced by 20% to 25% due to operational considerations.	NERC : Per NRC, nuclear units must be Y2K compliant by 7-99 or be remped off-line.	Moderate depending on demand and reserves; could be high impact on nuclear-heavy areas with constrained transmission. Moderate to high. 4 nuclear plants in the WSCC totaling about 8500 MW. Concerns about the security of off-site power. If shut down, it takes several days to start back up. Limited mode of operation due to license constraints.	Carry sufficient reserves in the NW Prepare load curtailment plans Prepare back-up communication plan Minimize scheduled transmission outages.	Bring additional units on-line Implement load curtailment plans Implement back-up communication plan Use any reserved transmission capacity. Provide additional reserve margin if possible.
Generation (Power Supply)	G2	Extreme Light Load	External	Will enough 24 hour businesses shut down on New Years Eve (to avoid the risk unplanned shutdowns) so that we get extremely light loading conditions?	Initial hours of Y2k cut over dates; may extend days.	Low to moderate	WSCC	Moderate	Specific request for shutdowns on Jan. 1, 2000.	Report to scheduling.
Generation	G3	Extreme weather in the NW, heavy imports to the NW and Canada. Loss of Northwest generation coupled with loss of transmission to the NW. Plus loss of voice and data communication.	External	Extreme cold conditions exist in the NW. Transmission has been reduced to operate below RAS arming levels. Assume high Northwest import conditions. Loss of 5% hydro, 10% thermal and X% IPP/Cogeneration generation in the NW. Loss of a key transmission path (Loss of Path 15, Borah West, COI, Montana to NW).	Initial hours of Y2k cut over dates; may extend days.	Low to moderate	WSCC	Default to curtailment plan.	Carry sufficient reserves in the NW Prepare load curtailment plans Prepare back-up communication plan Minimize scheduled transmission outages.	Bring additional units on-line Implement load curtailment plans Implement back-up communication plan Use any reserved transmission capacity. Provide additional reserve margin if possible.
Generation (Power Supply)	G4b	Generator Tripping	Internal		Initial hours of Y2K transition.	High probability of less than [10%]* loss of generation; low probability of [10%] loss for Cogen.	Generation division	Low impact; location dependent impacts; concern is loss of more than reserve capacity.	Checking all Cogen systems for Y2k problem.	
Generation (Power Supply)	G5b	Inability to Start or Restart Generators.	Internal	During the Y2K transition. Idle generators or those that trip off line are unable to start. On Monday loads will pick up. Transmission restrictions will be gone. Nuclear or other generation is not back on line. Is there enough generation to carry load?	Inability to start generation may be over an extended period before and after Y2k dates.	High probability of [15%]* or less unable to return to service as planned.	WSCC	Low to moderate impact; could be locally high impact. Units will be off line because of light load. Danger of not being able to start up when needed for heavy load Start-up controls are more complex than running controls.	During the Y2K transition, operate base loaded plants @ reduced output. Gives you more regulation capability. For nuclear plants, operating at reduced levels avoids emergency turbine trips which allows you to get them on line sooner Have load curtailment plans in place.	Implement load curtailment plans. Request external resources.
Generation (Power Supply)	G6	Loss of Generation - Thermal, Nuclear, Hydro.	External	Determine how many large plants in Mountain Time Zone can WSCC lose until regional or widespread problems occur. Determine how many large plants in Pacific Time Zone can WSCC lose until regional or widespread problems occur. Which units cause the most problems?	Initial hours of Y2k cut over dates; may extend days.	Low probability. See G5	WSCC	Low to moderate impact; could be locally high impact. Units will be off line because of light load. Danger of not being able to start up when needed for heavy load Start-up controls are more complex than running controls.	Maintain additional generating capacity on line, including older units with analog controls, and carry additional spinning reserve to enable recovery from various contingencies. To the extent possible, defer planned maintenance outages on generation equipment to ensure maximum availability during critical periods.	Verify if Generia 1 and 2 need to be at spinning reserve.

EXHIBIT F

Area	#	Risk	Problem Origination	Description	Period	Probab.	Source of Assumption	Impact	Prevention Strategies	Mitigation ...tegies
Generation ***(Power Supply)***	G7	Loss of multiple generation plants in the Pacific Time Zone following loss of Mountain Time Zone thermal generation. Plus loss of voice and data communication.	Compound	This occurs during the 2nd hour of the Y2K event. Pacific time zone reserves may have covered the loss of Mountain time zone generation. Assume that the system is in balance. However, some entities may be short generation and not know it due to loss of data. Remaining Mountain time zone plants are at capacity. Now, Pacific time zone generation trips off.	Initial hours of Y2k cut over dates; may extend days.	Low probability. See G5	WSCC	Low to moderate impact; could be locally high impact. Units will be off line because of light load. Danger of not being able to start up when needed for heavy load Start-up controls are more complex than running controls.	Carry sufficient reserves in both time zones.	Verify if Generia 1 and 2 need to be at spinning reserve
Generation ***(Power Supply)***	G8b	Loss of Multiple Generators.	External	Assume loss of 5% loss of hydro generation, 10% thermal generation and ? % IPP/cogen generation.	Initial hours of Y2k cut over dates; may extend days.	Low probability.	WSCC	Low to moderate impact; could be locally high impact. Units will be off line because of light load. Danger of not being able to start up when needed for heavy load Start-up controls are more complex than running controls.	Evaluate impacts Have load curtailment plans in place Carry additional spinning and ready reserves. Optimize hydro system to provide maximum system benefit.	Utilize Pump Storage in California Implement load curtailment plans. Shed load. See G6
Generation ***(Power Supply)***	G9	Loss of multiple thermal generation plants in Mountain Time Zone. Plus loss of voice and data communication.	External	The year 2000 event in the WSCC will impact the Mountain Time Zone first. Thermal generation in Colorado, Montana, Wyoming, Utah, and Arizona begin tripping off-line. Transfers to the NW are interrupted.	Initial hours of Y2k cut over dates; may extend days.		WSCC		Carry sufficient reserves in both time zones Prepare load curtailment plans.	
IT	IT1a	Application Software	Internal	Utility Billing and Financial	Days to weeks	Low	SVP Project Team	Moderate impact for interest payments.	Analyze, fix and test. Replace and upgrade where needed.	Manual operations Upgraded to Y2k NT4 and Office 97
IT ***(SCADA/Operations)***	IT4b	Application Software	Internal	Process Control	Initial hours of Y2k cut over dates; may extend days.	Low	SVP Project Team	Moderate	Upgrade operating software UNIX ver. 4d and ABB Spider ver. 8 to be in compliance.	Upgrade
IT ***(Energy Dist.)***	IT5	Control Center Failure or loss of facilities	Internal	Control Center Failure or innaccessable, unuseable or destroyed facilities	Initial hours of Y2k cut over dates; may extend days.	Low	WSCC	Moderate to high impacts. The impact can be high if the problem persists and higher loads are being encountered.	Prepare back-up control center procedures. Duplicate mapping and other Control Room tools.	Switch to back up control center or implement other back up procedures.
IT ***(SCADA/Operations)***	IT6	EMS/SCADA failure	Internal	Loss of SCADA blinds operations and causes loss of remote operation. Loss of Daytel impacts scheduling.	Initial hours of Y2k cut over dates; may extend days.	Moderate probability of loss of some EMS/SCADA functions. Scheduling functions may be at higher risk. moderate-buffer overload; low to moderate of communication bad data.	NERC, WSCC, and SVP Project Team	Moderate impact if combined with other contingencies. Restoration will take much longer without EMS or critical data.	Procedures should be developed to allow operators to acquire sufficient information to be able to run their system correctly.	Implement procedures to operate the system manually.
IT ***(Fuel Supply)***	IT7b	Interface Management	Internal/External	Electronic data interchange (EDI) Supplier payments disrupted, resulting in shortages of goods and services.	Initial hours of Y2k cut over dates; may extend days.	Moderate to high	SVP staff finance	Low	Analyze, fix, and test interfaces internal and external. Have back up supply on hand. Contract with vendors.	Write checks manually or other wise implement pre-electronic procedures.
IT	IT8	IT Infrastructure	Internal	Hardware failures	Initial hours of Y2k cut over dates; may extend days.	Low to moderate	WSCC and SVP Project Team	Low to moderate	Analyze, fix and test. Replace and upgrade where needed.	Use alternate equipment. Fix on failure
IT ***(Data Mgmt.)***	IT9b	Loss of critical operating data or incorrect data (ie line data, generation data, etc.).	Internal	Hubs, routers, gateways, switches, database, application, print servers.	Initial hours of Y2K transition.	Moderate probability of loss of some operating data.	Correlates with EMS/SCADA failure.	Moderate impact depends on telemetry data.	Analyze, fix and test. Replace and upgrade where needed.	Have Y2k compliant 3Com hubs and routers.
IT ***(SCADA/Operations)***	IT10	Loss of functionality within an energy management system.	Internal	Hardware and software	Initial hours of Y2k cut over dates; may extend days.	Moderate probability of loss of some operating data.	WSCC	Moderate impact depends on telemetry data.	Analyze, fix and test. Replace and upgrade where needed.	

EXHIBIT F



Area		Risk	Problem Origination	Description	Period	Proba.	Source of Assumption	Impact	Prevention Strategies	Mitigation .. .tegies
IT *(Data Mgmt.)*	IT11a	Meter data translation systems.	Internal	Hardware and software	Initial hours of Y2k cut over dates; may extend days.	Low; not time dependant.	SVP Project Team	Moderate depending on data loss.	Analyze, fix and test. Replace and upgrade where needed.	Manual data record
IT *(Data Mgmt.)*	IT12b	Power Quality Monitoring	Internal	Hardware and software	Initial hours of Y2k cut over dates; may extend days.	Low	SVP Project Team	Moderate	Analyze, fix and test. Replace and upgrade where needed.	
IT *(Data Mgmt.)*	IT13	Records	Internal	Hardware and software	Initial hours of Y2k cut over dates; may extend days.	Low	SVP Project Team	Low. Backed up by tape and hard copy.	Analyze, fix and test. Replace and upgrade where needed.	Manual data record
IT *(Data Mgmt.)*	IT14	Shared databases and files	Internal	Data accessed by multiple areas. Tapes, floppy disks, forms, file transfer protocol (FTP).	Initial hours of Y2k cut over dates; may extend days.	Low. Oracle Database is Y2k compliant.	SVP Project Team	Low. Backed up by tape and hard copy.	Analyze, fix and test. Replace and upgrade where needed.	Manual data record
IT *(Data Mgmt.)*	IT15b	Wire Transfers	External	Unable to send or receive wire transfer to cover power trading activities. Inaccuracy of information and amounts.	Initial hours of Y2k cut over dates; may extend days.		SVP Project Team	High impact. If we stop paying people we will not be able to trade on margin.		
IT *(Data Mgmt.)*	IT16	Work products created through use of PC applications.	Internal	Spreadsheets created through Lotus, Excel, Dbase	Initial hours of Y2k cut over dates; may extend days.	Low. Y2k compliant.	SVP Project Team	Low to High	Analyze, fix and test. Replace and upgrade where needed.	Manual operations
Load *(Engergy Dist.)*	L1a	Remote switching	Internal	Several breakers	Two hours	Low	SVP Project Team	Moderate	Analyze and prepare for backup.	Standby crew.
Load *(SCADA/Operations)*	L1b	Load dispatch and remote switching controls and load management systems.	Internal	2 remote switches	Initial hours of Y2k cut over dates; may extend days.	Low probability	SVP Project Team	Low impact	N/A	N/A
Load *(Engergy Dist.)*	L2	Load Shedding failure (under-frequency and under-voltage) or false operation.	Internal	2 remote switches, several breakers and manual load shedding.	Initial hours of Y2k cut over dates; may extend days.	Moderate probability of inadvertent operation or failure to operate.	NERC and WSCC	High impact if failures do occur; large portion of loads susceptible to shedding; cascading outages; could be over generation condition if inadvertent load shedding with extra generation on. High impact if large portions of load are lost near simultaneously.	Knowledge of load conditions.	Manually close or open.
Load *(Engergy Dist.)*	L3	Loss of Load See L2	External	Loss of XX MW of DSI load in the NW. This occurs near simultaneously at light load conditions. High frequency is the concern.	Initial hours of Y2k cut over dates; may extend days.	High probability of some load loss. Low probability of load loss sufficient to impact bulk electric operations. Near simultaneous loss of Direct Service Industry (Interruptible) load in the NW could impact the grid. 10% most likely; 10% to 25% 2nd most likely. Plan for various levels up to 100% (not likely but possible).	WSCC and NERC	Low impact unless large amount of load is lost.	Evaluate impact on generation.	Reduce generation as needed Use available reactive devices to control high voltage problems.
Load *(Engergy Dist.)*	L4	Scattered Loss of Load and Uncharacteristic load patterns.	Internal	Loss of small blocks of load throughout the interconnection. High frequency is the concern.	Days leading to and after Y2k roll over dates.	Moderate to high probability of unusual load patterns.	WSCC and NERC	Low impact; consider possible effects on system flows. Low impact to bulk transmission system.	Have enough units on-line with sufficient regulation to maintain frequency.	Regulation in Units. If needed, drop units off line. Use available reactive devices to control high voltage problems.
Logistics *(Cash Flow/Payroll)*	LG1a	Unable to pay for immediate services,i.e. meals	Internal	Cash on Hand	Days to weeks	Low	SVP Project Team		Increase amount in Petty Cash and plan for estimated number of staff needed.	Use manual purchase orders; institute blanket purchase orders with local merchants.
Logistics *(Fuel Supply)*	LG2	Constrained supply of oil	External	Diesel for back up generation may not be available to replenish reserves. Fuel may not be available for vehicles.	Days to weeks	Low probability	NERC/SVP	High impacts on power supply	Top off fuel tanks and procure additional supplies as necessary.	Verify all storage tanks are full.

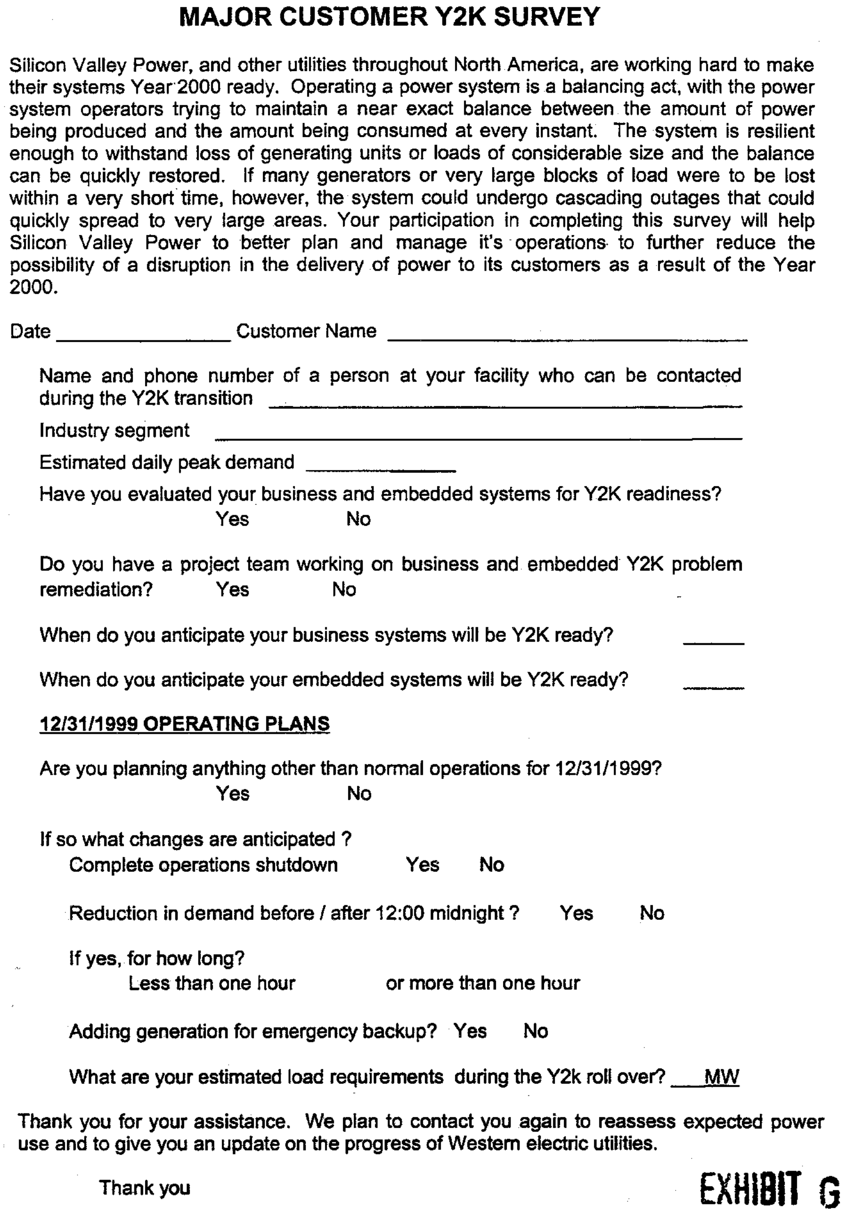
EXHIBIT F

Area	,	*Risk*	*Problem Origination*	*Description*	*Period*	*Probs.*	*Source of Assumption*	*Impact*	*Prevention Strategies*	*Mitigation . . ategies*
Logistics *(Logistics)*	LG4	Food	Internal	Suppliers of food may not be in operation.	Initial hours of Y2k cut over dates; may extend days.	Low	SVP Project Team	Moderate to high	Storage of food. Lease of catering trucks.	
Logistics *(General)*	LG8	Loss of supplies, including water.	Internal	No water for consumption, sanitation, etc.	Days to weeks or months.	Low probability	NERC	Low to moderate	Bottled water, storage of water, other sources.	
Logistics *(Logistics)*	LG9	Parts, equipment, materials.	Internal	Vendors may not be in operation, or may not have parts, equipment, materials needed.	Days to weeks	Low to moderate probability	SVP Project Team		Extra equipment and materials on hand.	
Logistics *(Fuel Supply)*	LG10a	Pipelines constrain supply or pressure of natural gas.	External	Natural gas used to provide generation may not be available.	Initial hours of Y2k cut over dates; may extend days.	Low to moderate probability	NERC	High impacts on power supply	N/A	Work with PG&E to restore service.
Logistics *(Power Supply)*	LG11	Rail systems constrain coal supply.	External	San Juan coal plant	Days to weeks or months	Low probability	NERC	Low short term; moderate long term.	Contact San Juan power plant management.	Contact San Juan power plant management.
Misc *(Data Mgmt.)*	M1	Document Control	Internal	Contracts, compliance letters, vendor responses, test results.	Days to weeks	Low	SVP Project Team	Low	Collect and maintain to ensure coordination and to establish record of efforts in case of litigation.	Back Up copies on disc, electronic, and paper.
Misc *(Cash Flow/Payroll)*	M2	Electronic payroll deposit	Internal	Employee direct deposit may be late or fail.	Days to weeks	Low	WSCC	Low	Test interfraces	Write checks manually or pay in cash.
Misc *(Power Supply)*	M4	Impact of two time zones in the interconnection.	Compound	We don't have two time zones.	Initial hours of Y2K transition	Moderate to high probability of a loss of thermal plants in the Mountain Time Zone with a resulting interruption of transfers to the Northwest.	WSCC	High impact locally or in Northwest		
Misc *(Energy Dist. And Facilities)*	M5a	Sabotage	Internal/ External	Disgruntled employees or irate citizens.	Days during the key Y2K transition dates.	Low to moderate probability of incidents.	NERC and WSCC	Moderate to high for local impacts.	Have team do perimeter/security prior to event	Police/security to cover Plants.
Misc *(Energy Dist.)*	M6a	Severe weather conditions.	Compound	High winds, rain, lightening, cold.	Days leading up to and after Y2K transition.	Low to moderate -- varies	SVP Project Team	Low impact on loads and system flows under severe weather.	Routine maintenance and tree trimming.	Standby crew.
Misc *(Energy Dist.)*	M7	Streetlights	Internal/ External	Failure or malfunction of lighting on property owned or maintained by private entity or other government agency.	Initial hours of Y2k cut over dates; may extend days.	Low	SVP Project Team and WSCC	Increased risk of crime and driving hazards.	Routine maintenance and tree trimming.	Manual activation, if possible. Secure additional security personnel. Standby crew.
Misc *(Transportation)*	M9	Traffic Lights	Internal/ External	Failure or misoperation of signals on City, County and State maintained roadways.	Initial hours of Y2k cut over dates; may extend days.	Low	SVP Project Team	Increased risk of crime and driving hazards.		Manual activation, if possible. Secure additional security personnel. Standby crew.
Misc *(Data Mgmt.)*	M11b	Written (Copiers, fax machines)	Internal	May stop working.	Days to weeks	Low	SVP Project Team	Low	Assess, Remediate, and Test.	Postpone or use carbon copies if available.
OASIS	O1	Loss of OASIS Node(s)	Internal	N/A	Initial hours of Y2k cut over dates; may extend days.	Low probability per NERC. High probability that the Internet will go down per WSCC.	NERC and WSCC Task Force (note that this contradicts NERC).	Low impact, may cause confusion in electric markets and affect market prices.	Assess, Remediate, and Test.	Use other forms of communication
Personnel *(Personnel)*	P1	Insufficient staff	Internal	Availability of operating personnel and supporting staff due to holidays, transportation, scheduling. Overtime support and time trading. Need support and cooperation of unions to meet unusual staffing requirements and/or assignments.	Initial hours of Y2k cut over dates; may extend days.	Low to moderate	NERC and WSCC and SVP	Low to moderate	Maintain additional technical support staff at control centers to handle problems. This includes technicians, EMS personnel, programmers and engineers. Maintain additional operating personnel at control centers. This may include additional dispatchers, plant operators and switching personnel. Staff major generation and transmission substations that are normally operated only by remote control. Check contract language. Explore legal limitations. Work with union representatives and officials to p[repare for any eventualities.	

EXHIBIT F

Area		Risk	Problem Origination	Description	Period	Probability	Source of Assumption	Impact	Prevention Strategies	Mitigation Strategies
Transmission *(Power Supply)*	T1	Increased risk of transmission facility trips/near coincident unplanned outages.	Internal		Initial hours of Y2k cut over dates; may extend days.	Low probability of increased facilities tripping due to Y2k	NERC and findings of SVP staff.	High impact for multiple simultaneous outages; criticality is location specific.	Maintain inter-area transfers at relatively low levels to prevent cascading outages should transmission lines be forced out of service. To the extent possible, defer planned maintenance outages on transmission equipment to ensure maximum availability during critical periods. Ensure that all voltage control equipment is available. Prepare for isolated operation should it be necessary.	Have Generia units 1 and 2 at spinning reserve.
Transmission *(Power Supply)*	T2	Islanding and/or loss of transmission	External	Loss of power supply to receiving stations from PG&E.	Initial hours of Y2k cut over dates; may extend days.	Low	WSCC	High Impact as SVP cannot operate in an island condition.	Reduce schedules/OTC (transfers). This would be for an 9 hour block starting at 2200 hrs Mountain time and extending to 0600 hours Pacific time. Investigate the impact of a lines tripping. SLOW CLEARING OF FAULTS due to Loss of Transfer Trip Evaluate impact of reduced transfers against RAS misoperation.	Implement system restart procedures.

EXHIBIT F



MAJOR CUSTOMER Y2K SURVEY

Silicon Valley Power, and other utilities throughout North America, are working hard to make their systems Year 2000 ready. Operating a power system is a balancing act, with the power system operators trying to maintain a near exact balance between the amount of power being produced and the amount being consumed at every instant. The system is resilient enough to withstand loss of generating units or loads of considerable size and the balance can be quickly restored. If many generators or very large blocks of load were to be lost within a very short time, however, the system could undergo cascading outages that could quickly spread to very large areas. Your participation in completing this survey will help Silicon Valley Power to better plan and manage it's operations to further reduce the possibility of a disruption in the delivery of power to its customers as a result of the Year 2000.

Date ________________ Customer Name ________________________________

Name and phone number of a person at your facility who can be contacted during the Y2K transition ________________________________

Industry segment ________________________________

Estimated daily peak demand ____________

Have you evaluated your business and embedded systems for Y2K readiness?
Yes No

Do you have a project team working on business and embedded Y2K problem remediation? Yes No

When do you anticipate your business systems will be Y2K ready? ______

When do you anticipate your embedded systems will be Y2K ready? ______

12/31/1999 OPERATING PLANS

Are you planning anything other than normal operations for 12/31/1999?
Yes No

If so what changes are anticipated ?
Complete operations shutdown Yes No

Reduction in demand before / after 12:00 midnight ? Yes No

If yes, for how long?
Less than one hour or more than one hour

Adding generation for emergency backup? Yes No

What are your estimated load requirements during the Y2k roll over? ___MW

Thank you for your assistance. We plan to contact you again to reassess expected power use and to give you an update on the progress of Western electric utilities.

Thank you

EXHIBIT G

Electric Utility Y2K Links

http://www.euy2k.com/
Rick Cowles is widely considered the leading Y2K authority on electric utilities and the year 2000. Covers many significant issues including Power Delivery, Nuclear Generation, Fossil Generation, Distribution, Embedded Controls, Deregulation/Y2K, Customer Service, Business Impact, Communications, Industry Status and Contingency Planning.

http://ourworld.compuserve.com/homepages/roleigh_martin/utilinks.htm
Roleigh Martin explains Y2K and the power utilities.

http://www.nerc.com/~y2k/y2kplan.html
NERC (North American Electric Reliability Council)Y2K Plan.

http://www.eei.org/EEI/press/y2k/
Edison Electric Institute.

http://www.y2ktimebomb.com
Westwergaard site offers a series of articles by various of Y2k experts. Powerful Prognostications by Dick Mills provides insightful and well-researched articles on the electric industry.

http://www.cpuc.ca.gov/Y2K/
Information regarding the California Public Utility Commission regulated utilities which includes essential telecommunications, energy, water, and transportation services throughout California.

http://www.appanet.org
Site of the American Public Power Association the national trade association representing more than 2000 municipal and other state and local government owned electric utilities.

EXHIBIT H

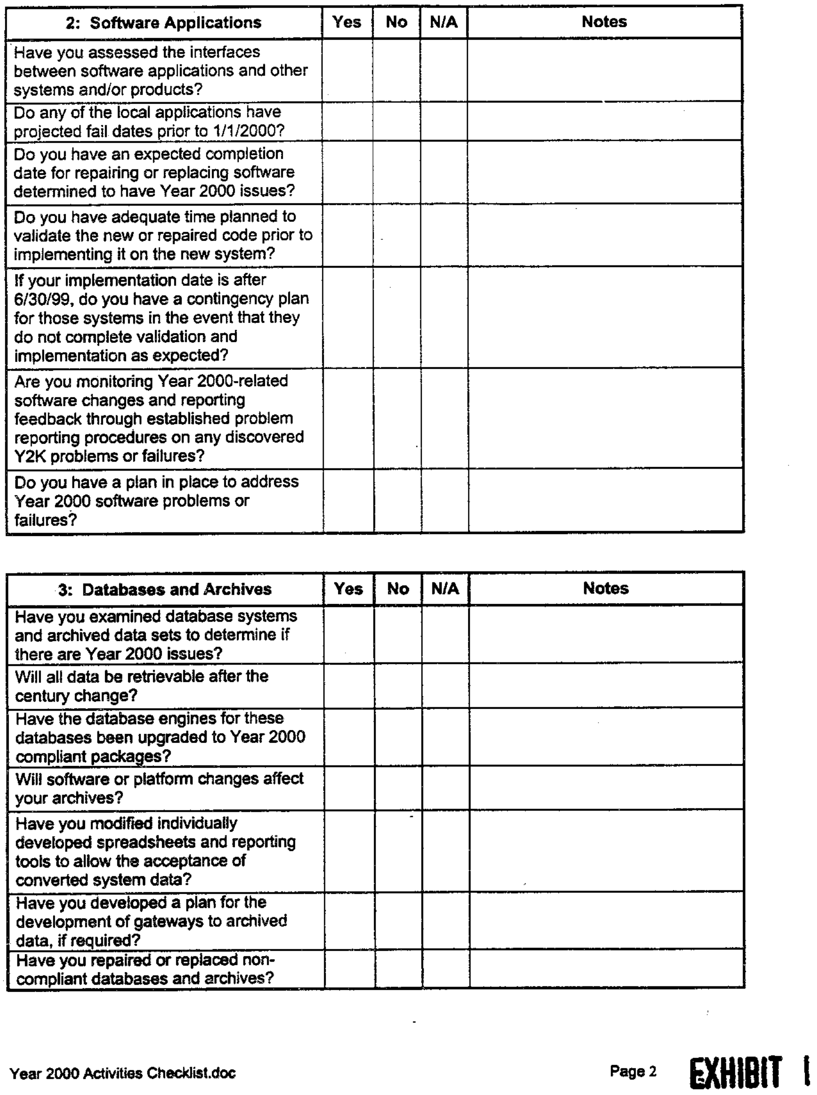
Year 2000 Activities Checklist

This document provides a checklist of activities and responsibilities related to conducting the Year 2000 readiness process. It is based on a Veterans Administration facilities checklist. It is not intended to be an all-inclusive compliance certification checklist that covers all affected systems and equipment, but rather a project management check sheet for Year 2000 activities network.

Related to Year 2000 Compliance of System/Product Areas:

1. General	Yes	No	N/A	Notes
Have you established a Y2K task force or working committee?				
Does this committee meet at least monthly?				
Have written minutes been maintained for each meeting of the committee?				
Has Y2K been given high priority for resource allocation?				
Have you incorporated Year 2000 certification requirements in the purchase or maintenance of your equipment and systems?				
Have you documented and kept on file compliance information received from manufacturers?				
Do you have a readily available inventory of systems at each hospital and does it include all systems/components that contain digital controls?				
Does your inventory include equipment in storage, out for repair, or being repaired internally?				
Have you developed and executed testing and implementation plans?				
Are you regularly checking Year 2000 Intranet web sites for updated information?				
Have you tested upgraded versions of your systems?				
Have you included Y2K failure scenarios in disaster drills?				
Have Y2K efforts and status been publicized to employees?				

EXHIBIT



2: Software Applications	Yes	No	N/A	Notes
Have you assessed the interfaces between software applications and other systems and/or products?				
Do any of the local applications have projected fail dates prior to 1/1/2000?				
Do you have an expected completion date for repairing or replacing software determined to have Year 2000 issues?				
Do you have adequate time planned to validate the new or repaired code prior to implementing it on the new system?				
If your implementation date is after 6/30/99, do you have a contingency plan for those systems in the event that they do not complete validation and implementation as expected?				
Are you monitoring Year 2000-related software changes and reporting feedback through established problem reporting procedures on any discovered Y2K problems or failures?				
Do you have a plan in place to address Year 2000 software problems or failures?				

3: Databases and Archives	Yes	No	N/A	Notes
Have you examined database systems and archived data sets to determine if there are Year 2000 issues?				
Will all data be retrievable after the century change?				
Have the database engines for these databases been upgraded to Year 2000 compliant packages?				
Will software or platform changes affect your archives?				
Have you modified individually developed spreadsheets and reporting tools to allow the acceptance of converted system data?				
Have you developed a plan for the development of gateways to archived data, if required?				
Have you repaired or replaced non-compliant databases and archives?				

EXHIBIT I

4: COTS Software	Yes	No	N/A	Notes
Have you required Year 2000 compliance information on all new COTS software purchases?				
Have you regularly checked the manufacturers' Year 2000 Intranet site to determine COTS software compliance information for applications that you own?				
Are software platform upgrades complete?				
Have interfaces between systems and devices been identified and corrected if necessary?				
Have you repaired or replaced non-compliant software?				

5:Computer Systems	Yes	No	N/A	Notes
Have you incorporated Year 2000 compliance requirements in the purchase of new equipment and services and for the correction and maintenance of existing systems?				
Have you repaired or replaced non-compliant systems?				
Have you tested all personal computers in your network for Y2K compliance?				
Have you replaced or repaired non-compliant equipment?				
Are you aware that Year 2000 issues extend to file servers and networks, and that you must incorporate these products in your scope of equipment assessed for Year 2000 problems?				
Is Year 2000 compliance is incorporated into all contracts for COTS software and hardware acquisitions?				
Are you regularly checking the manufacturers' Internet web site for COTS hardware compliance information?				
Are hardware platform upgrades complete?				

EXHIBIT 1

6: Facility-Related Systems	Yes	No	N/A	Notes
Are you addressing the problems of facility systems where update software may only be purchased from one vendor at vendor's name prices?				
Have you documented implementation of compliant facility-related systems?				
Are you checking the GSA web site at http://globe.lmi.org/lmi_pbs/y2kproducts/ for updated facility-related information?				
Have you planned an Emergency Preparedness Drill, including the Y2K scenario?				
Will you complete your emergency electrical system test by August 31?				
Are you tracking information concerning manufacturers who are charging large sums of money for updates to non-compliant utility components and systems?				

7. Other	Yes	No	N/A	Notes
Have you accurately tracked and reported all costs incurred by Y2K compliance activities?				
Have you been assured by EDI trading partners regarding compliance of electronically exchanged date formats?				
Are vendor compliance and related issues well documented?				
Is your legal counsel involved in vendor assurance and other aspects of your Y2K project, specifically relating to contract issues and potential tort claims?				

1. Business Continuity and Contingency Planning (BCCP)	Yes	No	N/A	Notes
Have you designated a Business Continuity Planning Workgroup and assigned responsibilities?				
Have you conducted an assessment of mission critical systems and processes?				
Has the assessment been reviewed by the BCPW to determine risk and priority?				
Have you generated a schedule to track critical events?				

EXHIBIT I

1. Business Continuity and Contingency Planning (BCCP)	Yes	No	N/A	Notes
Have you developed, published and distributed the Contingency Plan?				
Does your plan identify who has the authority/responsibility to activate and deactivate the plan?				
Does your plan articulate triggers for activating and deactivating the plan?				
Have you trained staff for BCCP responsibilities?				
Have you tested the plan?				
Have you critiqued and evaluated the tests?				
Have you modified the plan based on lessons learned?				
Has the BCPW reviewed all aspects of the contingency plan for facility-wide consistency and coordination?				
Have you reviewed all contingency plans for City-wide consistency and coordination?				

2. General	Yes	No	N/A	Notes
Have business partners been assigned a level of risk (i.e. failure of supplies of water, telephone, and power)?				
Have you communicated with local emergency planning committees regarding Y2K contingency plans?				
Have you communicated with area utilities regarding contingency plans?				

3. "Zero Hour" Plan	Yes	No	N/A	Notes
Do you have a plan for handling leave requests and mandatory overtime?				
Have you planned which staff will be present during the critical period 72 hours before and after the New Year?				
Have you planned what resources will be available to workers?				
Do you have specific operational procedures planned for the evening of December 31, 1999?				

EXHIBIT 1

3. "Zero Hour" Plan	Yes	No	N/A	Notes
Have you planned which equipment will be allowed to remain on during the rollover?				
Have you developed an Execution Phase Timeline or similar plan for the critical period surrounding the Year 2000 rollover?				

EXHIBIT I

Mr. HORN. Our next witness is Dr. Frances Winslow, the director of the Office of Emergency Services, city of San Jose. Nice to have you here.

Ms. WINSLOW. I guess it's still good morning. We appreciate your coming to visit us.

Mr. HORN. Not by my watch. It's afternoon now. One of us is wrong. This has been on my wrist for 50 years, so who knows.

Ms. WINSLOW. We appreciate the opportunity to have you come to us here in Silicon Valley to discuss the topic that perhaps is of greater interest here than in other parts of the country, because not only are we consumers, but as you heard from our previous panel, our economic base is greatly involved with the high-tech community. I brought a formal testimony which I know that you received, so I'd like to make a few informal remarks to you here instead.

Earlier one of the panel members mentioned the impact the media has had and how unfortunately the coverage is perhaps not what we might have hoped. But I've been encouraged to see in the last couple of weeks an increasing amount of interest in the media. I brought a couple of examples today. I'm a member of the American Planning Association. They have a whole article on what planners can do to prepare. I'm sorry I didn't have it last July instead of this July, but I guess better late than never. Also there's a publication called Emergency Preparedness News that covers hurricanes and FEMA and terrorism, and now also Y2K readiness, and then here is the Kiwanis Club's most recent magazine, and one of their cover stories is Y2K.

Why do I mention this? Because one of the biggest parts of my job is dealing with the community here and answering questions that citizens have about emergency preparedness. Five years ago most of the questions were: What do I do if there's an earthquake? But in the last 12 months most of the questions have been: What do I do on December 31st? But it's been an opportunity for my office to benefit, because it was very hard to get people interested in things they think would never happen like big earthquakes. But they see a date, and they have something to focus on.

I think for us in the emergency management community, Y2K has actually been a benefit because it helped us to get our community aware of the need to be prepared, not only for Y2K, but for the earthquakes that we know are inevitable in the area. We have three faults. And also for the winter storms that we have unfortunately on a repeated basis, and other kinds of natural, technological and man-made disasters that could potentially occur in our community.

And so the message that we're trying to send is that if you're prepared for a major earthquake, you're prepared for Y2K, because our estimate is that the most direct impact Y2K may have on the average community could be some temporary infrastructure blips that will be rather quickly remedied, but if people are unaware of what they might be, they could become frightened. Whereas by trying ahead of time to make them aware of some of the potential issues and also the things they can do to deal with those issues, we hope to lower the stress level, prevent anyone from feeling a sense of panic, and help them to be reassured that we are all living in a technological society, and sometimes things don't work.

We are fortunate in our community to have a group of very dedicated volunteers. We call them "San Jose Prepared!" They're a community emergency response team. We're part of FEMA's nationwide effort in this field, and our team is growing every quarter as we add new trained folks. But right now we have over 500 members who are scattered throughout the community of over 900,000 community members. They have received 16 hours of training and gone through a 2-hour exercise. It's usually an earthquake scenario, but it gives them some confidence that they can deal with unexpected disasters. We also equipped them with some skills, so that if our normal public safety systems are temporarily overwhelmed they can begin to provide some of those services to their own neighbors in their own communities until professionals are able to triage them into the system.

That group began preparing actively in January of this year for Y2K, and in the packet that I gave you, you have a copy of the Y2K newsletter that we distributed to those folks. They're our ambassadors throughout the community. They contact their own neighbors and friends and pass this word along. In addition, we have a website for our group, and one of the elements on our website is the Y2K page so that they can refer neighbors and friends who are computer oriented to get this information for themselves.

The American Red Cross also followed this spring with the creation of a brochure, and I've given that to you as well, and that's available on the American Red Cross website. That's another place where people can go to get basic personal preparedness information which is good not only to get through January, but also for the potential of earthquakes and floods in the future.

The other part of my office's responsibility, however, is to the internal organization of the city of San Jose to assist departments in developing contingency plans and to maintain the emergency operation center for the city. In order to help those who might be working in the EOC, we have worked with Mark Burton and others to develop some exercises and testing opportunities for the city staff.

We began with what we call a facilitated discussion where the leaders of the various departments came together to say what they thought their plans were, and we thought it was very important for them to hear each other, because some plans interacted with other plans, and if everybody plans to use the same generator at the same time, that was going to be a problem. So the facilitated discussion allowed us to begin to review what kind of plans each department had and how they might interact with other departments with the goal of being able to support each other through this time period.

In addition, we have a tabletop exercise scheduled for just a couple of weeks which, now building on the facilitated discussion, we hope will allow us to have a much smoother plan, one that will be fully integrated and where all of the support pieces are in place. However, we have also scheduled a third one for October to make sure as a kind of second test that the plans are working, that the expectations have been fulfilled, and we are scheduling this in the middle of the month of October so that if there are still last minute things that need to be cared for, there's an adequate timeframe available for the departments to do any last minute procurement or planning for personnel staffing before the time comes when they need to be activated.

In most communities, New Year's Eve is a busy time for the public safety community just because people like to go out and party; they drive around sometimes when they shouldn't be driving, and they create a certain level of demand for medical services, police services and other kinds of response services under very ordinary New Year's conditions. This year isn't an ordinary New Year. Most people unaware of history really do think that this is some sort of a turn of the millennium or some sort of cataclysmic date, and so there are plans for big parties, big religious celebrations and other kinds of big community gatherings. So in the downtown, we have the potential to have more people than usual present in one area at one time. In addition it's winter, and as part of California that can mean rain and sometimes very heavy rain.

And then finally, of course, everything that we do on New Year's Eve depends on infrastructure. We expect the roads to get us there and get us home. We expect the food suppliers to have the food and the water suppliers to have the water and the electricity to stay on so the band can play. And if all those things continue as we hope they will, it will just be a bigger than usual New Year's Eve party, and the community will wake up on the 1st with a happy feeling, and we will all have enjoyed being together on New Year's Eve.

But because we have to be prepared for things to go less than optimally, we have a plan to open our emergency operation center at 3:30 p.m. Initially it will be staffed by our amateur radio operators who will be communicating with their colleagues in Australia, New Zealand, Japan, other parts of Asia and Europe, places where Y2K will have already been experienced or will be in the process of being experienced. We hope to be able to learn something from that surveillance that may assist us in last minute preparations. In addition, we will have our emergency public information officers present to survey the media to see what kind of information is being given out to the public by the media, and to see how the East Coast cities will experience the event first and are discussing their issues.

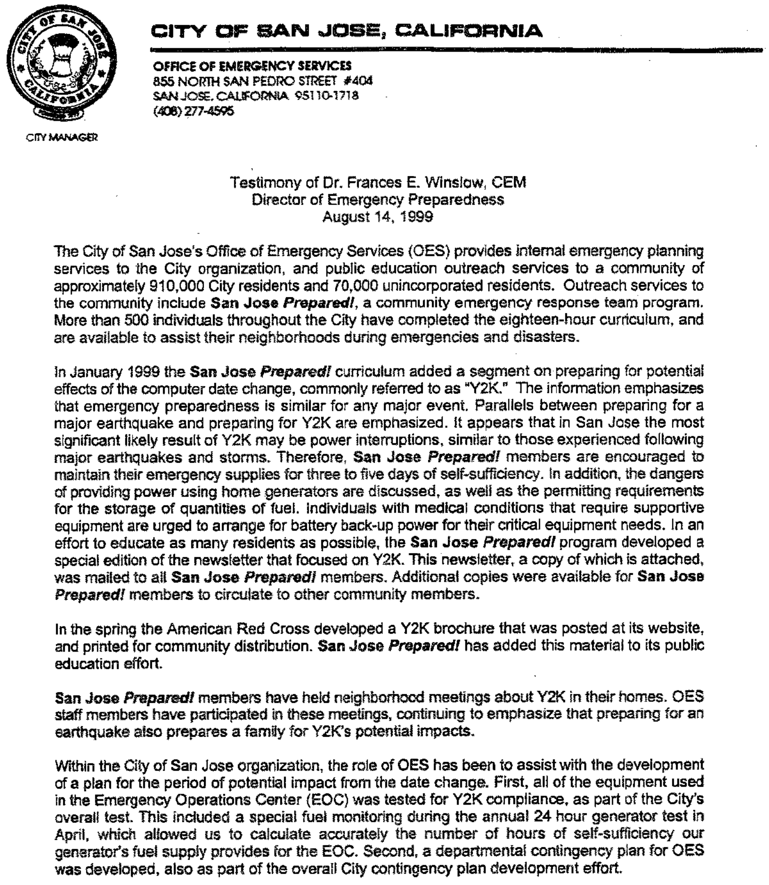
At 8:30 we will have the members of the senior staff of the city of San Jose join the city manager in the Emergency Operation Center, and we will be there for as long as we are needed or until 8:30 the following morning, whichever comes first. If it turns out that issues occur that do require continued monitoring and presence, we will then be replaced for the next 12 hours by our executive staff of the city. I think this is important, for the Congress to be aware of the high level of importance that's placed on this event by the leadership of the city of San Jose. It's not the most junior person who gave up their New Year's Eve party with the family, but the most senior. And I think that that level of commitment is indicative of the level of commitment that exists throughout this organization, not only for Y2K, but for all events that can impact our community.

We have a help line that's always in place, 277–HELP. We've used it for many years during flood events in the winters. The public is familiar with it. This will be staffed to allow people who may have concerns or questions to easily reach us without impacting our 911 or 311 systems.

We hope that we're prepared, and we hope that our preparations turn out to have been an appropriate level of caution rather than a needed event. Thank you very much for coming to visit us, and we hope you'll come back sometime when you can just have fun.

Mr. HORN. Thank you very much, Dr. Winslow.

[The prepared statement of Ms. Winslow follows:]



CITY OF SAN JOSE, CALIFORNIA

OFFICE OF EMERGENCY SERVICES
855 NORTH SAN PEDRO STREET #404
SAN JOSE, CALIFORNIA 95110-1718
(408) 277-4595

CITY MANAGER

Testimony of Dr. Frances E. Winslow, CEM
Director of Emergency Preparedness
August 14, 1999

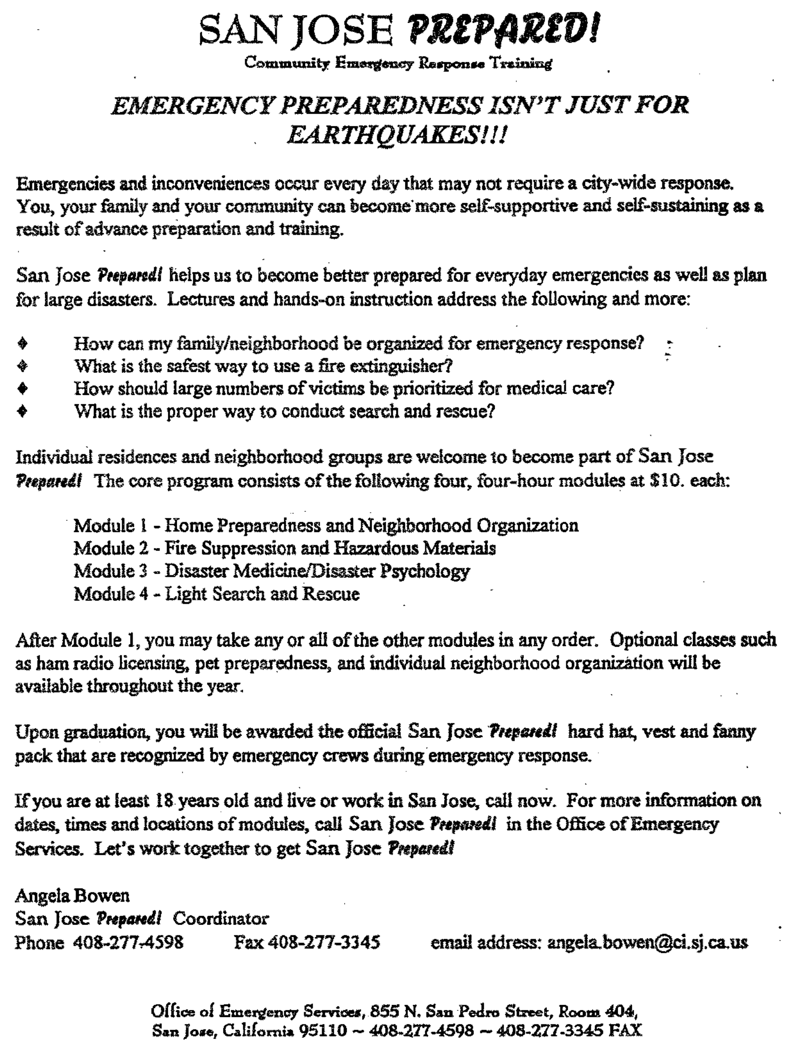
The City of San Jose's Office of Emergency Services (OES) provides internal emergency planning services to the City organization, and public education outreach services to a community of approximately 910,000 City residents and 70,000 unincorporated residents. Outreach services to the community include **San Jose *Prepared!***, a community emergency response team program. More than 500 individuals throughout the City have completed the eighteen-hour curriculum, and are available to assist their neighborhoods during emergencies and disasters.

In January 1999 the **San Jose *Prepared!*** curriculum added a segment on preparing for potential effects of the computer date change, commonly referred to as "Y2K." The information emphasizes that emergency preparedness is similar for any major event. Parallels between preparing for a major earthquake and preparing for Y2K are emphasized. It appears that in San Jose the most significant likely result of Y2K may be power interruptions, similar to those experienced following major earthquakes and storms. Therefore, **San Jose *Prepared!*** members are encouraged to maintain their emergency supplies for three to five days of self-sufficiency. In addition, the dangers of providing power using home generators are discussed, as well as the permitting requirements for the storage of quantities of fuel. Individuals with medical conditions that require supportive equipment are urged to arrange for battery back-up power for their critical equipment needs. In an effort to educate as many residents as possible, the **San Jose *Prepared!*** program developed a special edition of the newsletter that focused on Y2K. This newsletter, a copy of which is attached, was mailed to all **San Jose *Prepared!*** members. Additional copies were available for **San Jose *Prepared!*** members to circulate to other community members.

In the spring the American Red Cross developed a Y2K brochure that was posted at its website, and printed for community distribution. **San Jose *Prepared!*** has added this material to its public education effort.

San Jose *Prepared!* members have held neighborhood meetings about Y2K in their homes. OES staff members have participated in these meetings, continuing to emphasize that preparing for an earthquake also prepares a family for Y2K's potential impacts.

Within the City of San Jose organization, the role of OES has been to assist with the development of a plan for the period of potential impact from the date change. First, all of the equipment used in the Emergency Operations Center (EOC) was tested for Y2K compliance, as part of the City's overall test. This included a special fuel monitoring during the annual 24 hour generator test in April, which allowed us to calculate accurately the number of hours of self-sufficiency our generator's fuel supply provides for the EOC. Second, a departmental contingency plan for OES was developed, also as part of the overall City contingency plan development effort.



SAN JOSE *PREPARED!*

Community Emergency Response Training

EMERGENCY PREPAREDNESS ISN'T JUST FOR EARTHQUAKES!!!

Emergencies and inconveniences occur every day that may not require a city-wide response. You, your family and your community can become more self-supportive and self-sustaining as a result of advance preparation and training.

San Jose ***Prepared!*** helps us to become better prepared for everyday emergencies as well as plan for large disasters. Lectures and hands-on instruction address the following and more:

- How can my family/neighborhood be organized for emergency response?
- What is the safest way to use a fire extinguisher?
- How should large numbers of victims be prioritized for medical care?
- What is the proper way to conduct search and rescue?

Individual residences and neighborhood groups are welcome to become part of San Jose ***Prepared!*** The core program consists of the following four, four-hour modules at $10. each:

Module 1 - Home Preparedness and Neighborhood Organization
Module 2 - Fire Suppression and Hazardous Materials
Module 3 - Disaster Medicine/Disaster Psychology
Module 4 - Light Search and Rescue

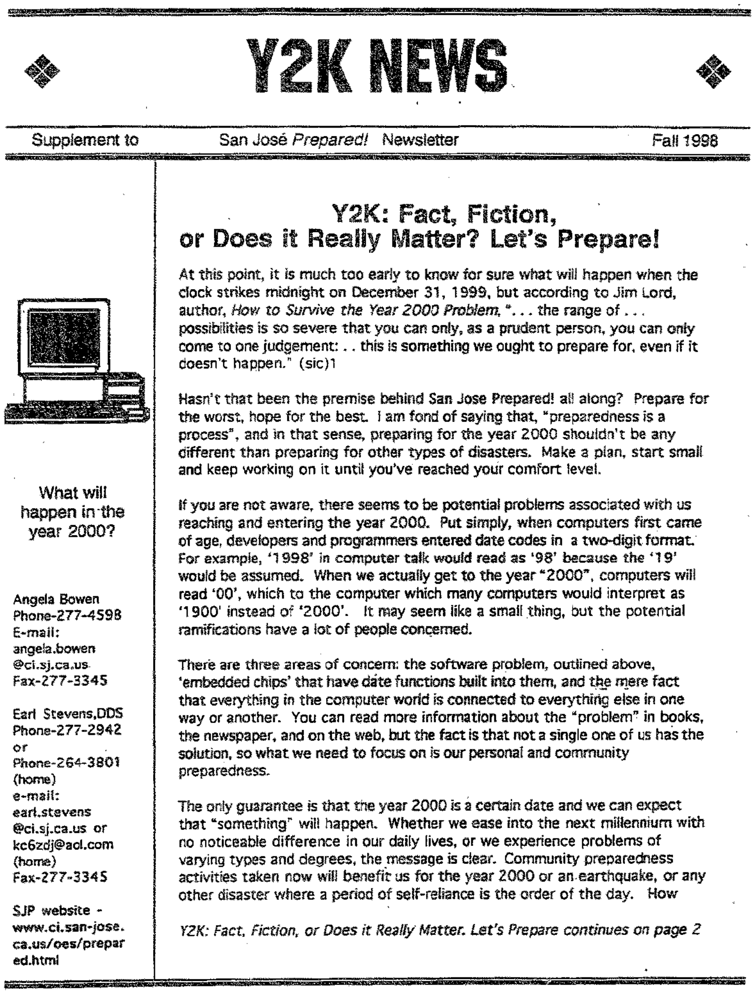
After Module 1, you may take any or all of the other modules in any order. Optional classes such as ham radio licensing, pet preparedness, and individual neighborhood organization will be available throughout the year.

Upon graduation, you will be awarded the official San Jose ***Prepared!*** hard hat, vest and fanny pack that are recognized by emergency crews during emergency response.

If you are at least 18 years old and live or work in San Jose, call now. For more information on dates, times and locations of modules, call San Jose ***Prepared!*** in the Office of Emergency Services. Let's work together to get San Jose ***Prepared!***

Angela Bowen
San Jose ***Prepared!*** Coordinator
Phone 408-277-4598 Fax 408-277-3345 email address: angela.bowen@ci.sj.ca.us

Office of Emergency Services, 855 N. San Pedro Street, Room 404,
San Jose, California 95110 ~ 408-277-4598 ~ 408-277-3345 FAX



Y2K NEWS

Supplement to San José *Prepared!* Newsletter Fall 1998

What will happen in the year 2000?

Angela Bowen
Phone-277-4598
E-mail:
angela.bowen
@ci.sj.ca.us
Fax-277-3345

Earl Stevens,DDS
Phone-277-2942
or
Phone-264-3801
(home)
e-mail:
earl.stevens
@ci.sj.ca.us or
kc6zdj@aol.com
(home)
Fax-277-3345

SJP website -
www.ci.san-jose.ca.us/oes/prepared.html

Y2K: Fact, Fiction, or Does it Really Matter? Let's Prepare!

At this point, it is much too early to know for sure what will happen when the clock strikes midnight on December 31, 1999, but according to Jim Lord, author, *How to Survive the Year 2000 Problem*, "... the range of ... possibilities is so severe that you can only, as a prudent person, you can only come to one judgement: .. this is something we ought to prepare for, even if it doesn't happen." (sic)1

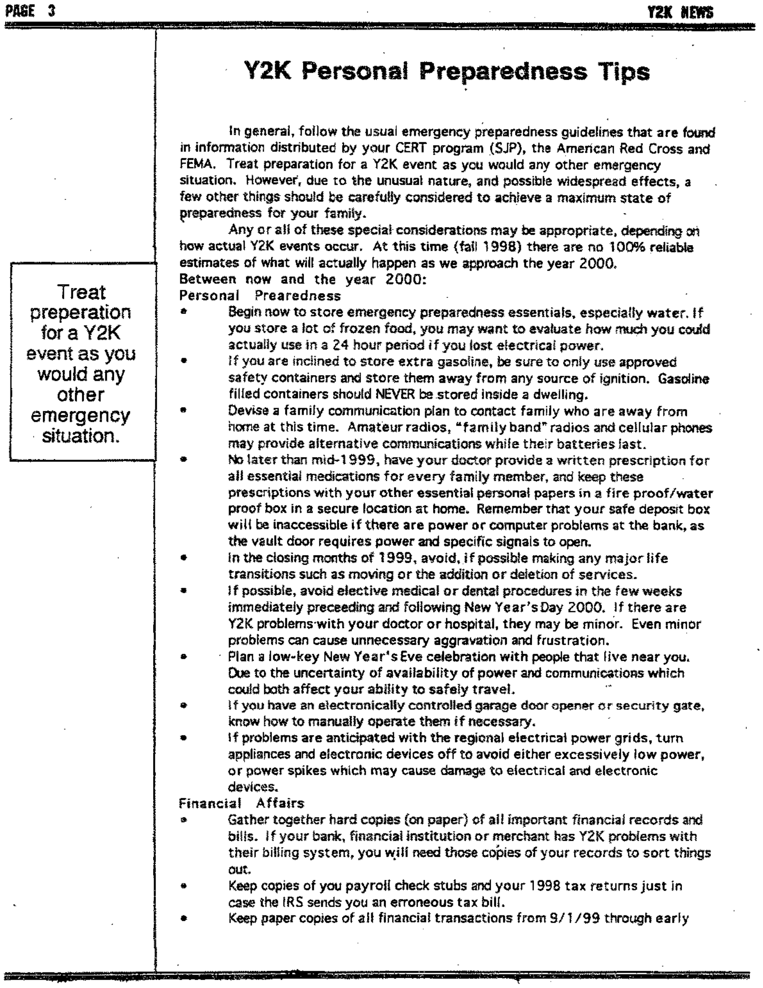
Hasn't that been the premise behind San Jose Prepared! all along? Prepare for the worst, hope for the best. I am fond of saying that, "preparedness is a process", and in that sense, preparing for the year 2000 shouldn't be any different than preparing for other types of disasters. Make a plan, start small and keep working on it until you've reached your comfort level.

If you are not aware, there seems to be potential problems associated with us reaching and entering the year 2000. Put simply, when computers first came of age, developers and programmers entered date codes in a two-digit format. For example, '1998' in computer talk would read as '98' because the '19' would be assumed. When we actually get to the year "2000", computers will read '00', which to the computer which many computers would interpret as '1900' instead of '2000'. It may seem like a small thing, but the potential ramifications have a lot of people concerned.

There are three areas of concern: the software problem, outlined above, 'embedded chips' that have date functions built into them, and the mere fact that everything in the computer world is connected to everything else in one way or another. You can read more information about the "problem" in books, the newspaper, and on the web, but the fact is that not a single one of us has the solution, so what we need to focus on is our personal and community preparedness.

The only guarantee is that the year 2000 is a certain date and we can expect that "something" will happen. Whether we ease into the next millennium with no noticeable difference in our daily lives, or we experience problems of varying types and degrees, the message is clear. Community preparedness activities taken now will benefit us for the year 2000 or an earthquake, or any other disaster where a period of self-reliance is the order of the day. How

Y2K: Fact, Fiction, or Does it Really Matter. Let's Prepare continues on page 2



Y2K Personal Preparedness Tips

In general, follow the usual emergency preparedness guidelines that are found in information distributed by your CERT program (SJP), the American Red Cross and FEMA. Treat preparation for a Y2K event as you would any other emergency situation. However, due to the unusual nature, and possible widespread effects, a few other things should be carefully considered to achieve a maximum state of preparedness for your family.

Any or all of these special considerations may be appropriate, depending on how actual Y2K events occur. At this time (fall 1998) there are no 100% reliable estimates of what will actually happen as we approach the year 2000.

Treat preperation for a Y2K event as you would any other emergency situation.

Between now and the year 2000:

Personal Prearedness

- Begin now to store emergency preparedness essentials, especially water. If you store a lot of frozen food, you may want to evaluate how much you could actually use in a 24 hour period if you lost electrical power.
- If you are inclined to store extra gasoline, be sure to only use approved safety containers and store them away from any source of ignition. Gasoline filled containers should NEVER be stored inside a dwelling.
- Devise a family communication plan to contact family who are away from home at this time. Amateur radios, "family band" radios and cellular phones may provide alternative communications while their batteries last.
- No later than mid-1999, have your doctor provide a written prescription for all essential medications for every family member, and keep these prescriptions with your other essential personal papers in a fire proof/water proof box in a secure location at home. Remember that your safe deposit box will be inaccessible if there are power or computer problems at the bank, as the vault door requires power and specific signals to open.
- In the closing months of 1999, avoid, if possible making any major life transitions such as moving or the addition or deletion of services.
- If possible, avoid elective medical or dental procedures in the few weeks immediately preceeding and following New Year's Day 2000. If there are Y2K problems with your doctor or hospital, they may be minor. Even minor problems can cause unnecessary aggravation and frustration.
- Plan a low-key New Year's Eve celebration with people that live near you. Due to the uncertainty of availability of power and communications which could both affect your ability to safely travel.
- If you have an electronically controlled garage door opener or security gate, know how to manually operate them if necessary.
- If problems are anticipated with the regional electrical power grids, turn appliances and electronic devices off to avoid either excessively low power, or power spikes which may cause damage to electrical and electronic devices.

Financial Affairs

- Gather together hard copies (on paper) of all important financial records and bills. If your bank, financial institution or merchant has Y2K problems with their billing system, you will need those copies of your records to sort things out.
- Keep copies of you payroll check stubs and your 1998 tax returns just in case the IRS sends you an erroneous tax bill.
- Keep paper copies of all financial transactions from 9/1/99 through early

AMERICAN RED CROSS
SANTA CLARA VALLEY CHAPTER
2731 N First Street
San Jose CA 95134
Disaster Info - (408) 577-2023
WEB SITE - http://www.redcross.org/ca/scv

American
Red Cross
We'll be there.

ARC 44801
Rev. Jan. 1999

Y2K

WHAT YOU SHOULD KNOW

American
Red Cross
We'll be there.

For more than 100 years, the American Red Cross has been at the cutting edge of disaster relief activities, helping people prevent, prepare for, and cope with disasters and other emergencies. That's why your Red Cross has published the following information about "Y2K"–its potential effects and what you can do to be prepared.

FREQUENTLY ASKED QUESTIONS

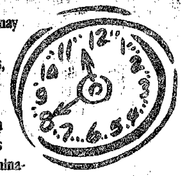
What is "Y2K" and why are people concerned?

The Year 2000 technology problem, or bug, as it is sometimes called, was created in the early days of computers, when memory in computers was scarce and expensive. Programmers took shortcuts whenever possible to save space. Instead of using a four-digit code for year dates, a two-digit entry was used. This practice persisted, long after the need for saving space was eliminated. The two-digit code also was used in embedded chips, which exist in many devices that control processes, functions, machines (like cars), building ventilation systems, elevators, and fire and security alarm systems, which are part of our everyday lives.

When the year 2000 comes, programs that have been coded with two-digit year codes will not distinguish between the years 2000 and 1900. If the program includes time-sensitive calculations or comparisons, results are unpredictable. No one knows what problems may occur, how widespread they may be, or how long they will last. The good news is that federal, state, and local governments; banks and other financial institutions; retail businesses, and every other group affected by this problem have been working to resolve it, and a great deal of progress has been made.

When could Y2K problems happen?

Most people anticipate Y2K problems may happen December 31, 1999, at midnight. Many experts predict that the problem is more likely to be a persistent one over a few years rather than a single "crash."

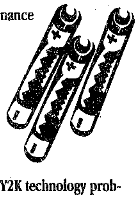


For example, there may be a computer-based problem with other dates, such as April 9, 1999, which is the 99th day of the year, or on 9/9/99. In the past, a series of nines was used to indicate termination of a computer program, and some experts believe that when all nines show up in a date sequence, some computer systems could read it as a program termination command.

There also is some concern regarding fiscal year 2000 dates in those organizations with fiscal years that start earlier than December 31, 1999. Also, the year 2000 is a leap year, and the leap year date 02/29/00 may be a problem for some computer programs as well.

What kinds of things could happen as a result of Y2K problems?

The President's Council on Y2K Conversion, established by the White House, as well as a special Senate Committee, have focused their attention on defining the scope of the Y2K problem. Hearings have been conducted by the United States Senate Special Committee on the Year 2000 Technology Problem and have focused on the following eight areas:



- Utilities and the national power grid
- International banking and finance
- Health care
- Transportation
- Telecommunications
- Pension and mutual funds
- Emergency planning
- General business

The potential effect of the Y2K technology problem on any of these areas is unknown, and the sit' ation continues to change as federal, state, and lc governments; industries; businesses; and organizations, as well as the general public, take actions to reduce the problem. Experts who spoke at the Senate hearings believe that there may be localized disruptions. For example, in some areas, electrical power may be unavailable for some time. Manufacturing and production industries may be disrupted. Roads may be closed or gridlocked if traffic signals are disrupted. Electronic credit card transactions may not be processed. Telephone systems may not work.

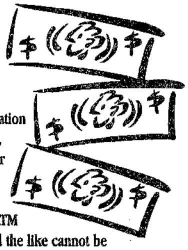
Because no one can be certain about the effects of the Y2K problem, the American Red Cross has developed the following checklist for you. These are s easy steps you can take to prepare for possible disruptions. All of these recommendations make good sense, regardless of the potential problem.

WHAT YOU CAN DO TO BE PREPARED

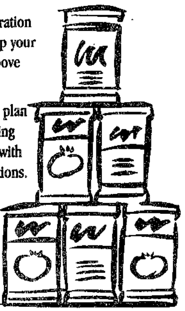
Y2K Checklist

___ Check with manufacturers of any essential computer-controlled electronic equipment in your home to see if that equipment may be affected. This includes fire and security alarm systems, programmable thermostats, appliances, consumer electronics, garage door openers, electronic locks, and any other electronic equipment in which an "embedded chip" may control its operation.

___ Stock disaster supplies to last several days to a week for yourself and those who live with you. This includes having nonperishable foods, stored water, and an ample supply of prescription and nonprescription medications that you regularly use. See *Your Family Disaster Supplies Kit* for suggestions.



___ As you would in preparation for a storm of any kind, have some extra cash or traveler's checks on hand in case electronic transactions involving ATM cards, credit cards, and the like cannot be processed. Plan to keep cash or traveler's checks in a safe place, and withdraw money from your bank in small amounts well in advance of 12/31/99.



___ As you would in preparation for a winter storm, keep your automobile gas tank above half full.

___ In case the power fails, plan to use alternative cooking devices in accordance with manufacturer's instructions. Don't use open flames or charcoal grills indoors.

___ Have extra blankets, coats, hats, and gloves to keep warm. Please *do not* plan to use gas-fueled appliances, like an oven, as an alternative heating source. The same goes for wood-burning or liquid-fueled heating devices that are not designed to be used in a residential structure. Camp stoves and heaters should only be used out of doors in a well-ventilated area. If you do purchase an alternative heating device, make sure it is approved for use indoors and is l ed with the Underwriters Laboratories (UL).

___ Have plenty of flashlights and extra batteries on hand. Don't use candles for emergency lighting.

___ Examine your smoke alarms now. If you have smoke alarms that are hard-wired into your home's electrical system (most newer ones are), check to see if they have battery back-ups. Every fall, replace all batteries in all smoke alarms as a general fire safety precaution.

___ Be prepared to relocate to a shelter for warmth and protection during a prolonged power outage or if for any other reason local officials request or require that you leave your home. Listen to a ıattery-operated radio or television for information about where shelters will be available.

___ If you plan to use a portable generator, connect what you want to power directly to the generator; do not connect the generator to your home's electrical system. Also, be sure to keep a generator in a well-ventilated area—either outside or in a garage, keeping the door open. Don't put a generator in your basement or anywhere inside your home.

___ Check with the emergency services providers in your community to see if there is more information available about how your community is preparing for any potential problems. Be an advocate and support efforts by your local police, fire, and emergency management officials to ensure that their systems will be able to operate at all times.

The American Red Cross helps people prevent, prepare for, and respond to emergencies. We're in your neighborhood every day, providing disaster preparedness information and teaching classes in first aid and other lifesaving skills, to help keep families like yours safer. For more information, please contact your *local* American Red Cross chapter. You can find it in your telephone directory under "American Red Cross" or through our home page at http://www.redcross.org—click on "Your Local Red Cross."

Mr. HORN. Pardon my ignorance, but what's a 311?

Ms. WINSLOW. I should probably let the chief answer that question.

Mr. HORN. How about it, Chief? You're next anyhow. We're delighted to have you.

Mr. LANSDOWNE. Thank you very much, Mr. Chairman. I'm Bill Lansdowne, and I'm very honored to be the police chief of this great city of San Jose. I intend to respect everybody's time and your time here in this meeting and follow the three "Bs" of testimony: Be right, be brief, and be quiet.

As it applies to our systems and our preparedness for the San Jose Police Department, community of San Jose, there are three major systems within police communications which handle police and fire calls. They are the telephones, the radio and the CAD system, and the telephones are two separate systems. One is the 911 emergency dispatch CAD system, and the other is 311, which is the non-emergency line. That is being monitored on a 24-hour basis, and takes some of the pressure off 911. There are three existing systems like that in the country. We were one of the pilot programs, and it's been very effective for us to really provide the best possible service.

Mr. HORN. What type of calls would you get on that 311 line? Do people really differentiate it?

Mr. LANSDOWNE. Very much so, Mr. Chairman. On the 911 line we get the emergency calls where there's a possibility of violence or a need for a emergency dispatch. Under 311 calls, we get the information for reports that can be taken at later dates, and many cases just information that the public wants to call in to the police department to determine or get an answer for.

Mr. HORN. Go ahead. I just wanted to learn what this was.

Mr. LANSDOWNE. Yes, sir. I would be delighted to give you a tour of our system. It's been very effective, and I think you'll see it's copied throughout the country.

Mr. HORN. Yes.

Mr. LANSDOWNE. The telephone and radio systems have been tested and are Y2K compliant, and the CAD system which is the backbone of the entire process, will be certified prior to January 1st, and we expect it to be certified very shortly. However, in the event of a partial or complete failure of any of the three systems and the expected calls for service, the following contingency plans have been developed and will be put into place for police services.

To provide for our ability to handle the expected increased calls for services, the communications personnel will be on 12-hour shifts for a 48-hour period to help us make a determination of what level of service that we need to continue to provide the community of San Jose. The telephone system has a backup failsafe system that allows the telephone calls to be rerouted to lines that will accommodate both emergency and non-emergency calls from the public.

Our dispatching of officers in the field can be converted to manual operation if the computer aided dispatch service loses power and begins to go down. In the event of a partial loss of radio power, our system has the ability to transfer units to other radio channels. In the event of a complete loss of radio power, we are prepared to use the portable radio systems referred to as the dispatcher-in-a-box system. This system is designed to be placed out at a remote location in the city, and will provide our communication link throughout the city of San Jose. The contingency plans to use five Fire Battalion stations also in place as remote transmitting locations.

As it applies to our police patrol staff, selected patrol division watches are scheduled to work 12-hour shifts for a 48-hour period. The Special Operations Division which is a very large section within our organization of the San Jose Police Department is being called back, and the officers are scheduled also to work 12-hour shifts, which will give us approximately 100 additional officers for that particular night to be available for calls for services.

Patrol staffing following New Year's Eve will be based on evaluation of the previous night's events. Similar to the other major events, the Police Department has a contingency plan to put in place 12-hour shifts. We have extensive experience for natural disasters here in the city of San Jose, and we can immediately go to emergency operation.

I'd like the assure this subcommittee and the community of San Jose that we have planned for the new millennium for the Y2K problem very well, and there is nothing that's going to happen that this city and this police department is not fully prepared to handle quickly and efficiently, providing that same level of service to this community that they have learned to expect, appreciate and demand.

And with that is my short comment.

Mr. HORN. Well, I appreciate it. Those were very succinct and to the point.

[The prepared statement of Mr. Lansdowne follows:]

Congress of the United States
House of Representatives
Subcommittee on Government Management, Information and Technology

"Is Silicon Valley Prepared for Y2K?"
Hearing on Year 2000 Readiness
Saturday, August 14, 1999
San Jose City Hall

Statement of William M. Lansdowne
Chief of Police
San Jose Police Department

Y2K CONTINGENCY PLANS AND PREPAREDNESS

Communications Systems

- There are three (3) major systems within police communications which handle police and fire calls for service. They are Telephones, Radio and CAD (Computer Aided Dispatch).

- The Telephone and Radio systems have been tested and are Y2K compliant, and the CAD system is expected to be tested and certified shortly.

- However, in the event of a partial or complete failure of any of the three systems, and the expected calls for service, the following contingency plans have been developed and will be put into place for police services:

  1. To provide for our ability to handle an expected increase in calls for service, communications personnel are scheduled to work 12-hour shifts from 12/31/99 to 1/2/00.

  2. The Telephone System has a backup system that allows telephone calls to be re-routed to lines that will accommodate both emergency and non-emergency calls from the public.

  3. Dispatching of officers in the field can be converted to manual mode of operation.

  4. In the event of a partial loss of radio power, our system has the ability to transfer police units to other radio channels.

Y2K CONTINGENCY PLANS AND PREPAREDNESS

5. In the event of a complete loss of radio power, we are prepared to use a portable radio system referred to as a "dispatcher-in-a-box" system. This system is designed to be placed out at remote locations around the city. They will provide our communication link throughout the city. The contingency plans to use the five Fire Battalion Stations as the remote locations.

Police Department Patrol Staffing

- Selected Patrol Division watches are scheduled to work 12-hour shifts starting 12/31/99 to 1/1/00.
- The Special Operations Division is being called back and the officers are scheduled to work 12-hour shifts starting 12/31/99 to 1/1/00. (approximately 100 officers)
- Patrol staffing following New Year's Eve will be based on an evaluation of the previous night's events. Similar to other major events, the Police Department has contingency plans to continue 12-hour shifts as needed.

Police Department Data Base Systems

- The San Jose Police Department is currently in the process of transitioning to an Automated Information System (AIS), which contractually must be Y2K compliant.
- The SJPD had ten (10) mission critical sub - systems requiring remediation or replacement to function in the interim until AIS is fully operational.
- Two of the systems are currently in their testing phase to ensure that they are compliant. All others have either been replaced or had remediation completed.

Mr. HORN. And your colleague from the fire department, John McMillan, deputy fire chief, city of San Jose, we're glad to hear from you.

Mr. MCMILLAN. Thank you, Mr. Chairman. Good afternoon and welcome, also your staff. We appreciate having you today, and I'm honored to have the opportunity to be a witness and speak for today.

San Jose Fire Department has evaluated mission-critical and mission-essential core services for our Y2K readiness in the city of San Jose. As of this submission, the department is confident that we will be able to fulfill our mission serving the citizens of San Jose. Fire department staff continues to evaluate these mission-related systems and processes and is developing a contingency method of service delivery in the event that any unforeseen Y2K problems should occur. We are specifically focusing on and making decisions in the following areas: One of the very interesting topics for us over the last 4 or 5 months is our defibrillators that we have on all of our advanced life support fire engines. It's a very good moment for me at this point in time, and Mark Burton mentioned it earlier, all 50 of our emergency medical defibrillators are now Y2K compliant. They all received two new embedded chips that will now allow those to be fully serviceable through the Y2K process.

We placed a hold on releasing all of our surplus fire apparatus. We are in good times. Over the last 5 years we purchased practically an entire fleet of new fire engines and aerial ladder trucks, but by buying these types of apparatus, we also were buying apparatus that's state-of-the-art and have a lot of embedded systems. To prepare for any unforeseen problems, we have not released any of our old apparatus we had. We are very proud to say today that we have 15 fire engines in reserve we're holding until well into the next year to see how we survive going through Y2K.

Mr. HORN. Just out of curiosity, were your old ones 2000 compliant?

Mr. MCMILLAN. Very good question, sir. What we can say is many of those apparatus were 1970's, early 1980's, that did not have the complex computer systems on them. They were the kind of apparatus that you or I might be able to open the hood of our car and change a spark plug or know where the distributor is. They're very basic, not really complicated, and they were apparatus we had around between 15 and 30 years, so we can't guarantee anything, but one thing we do know, that if anything goes down, we have a lot of equipment to back it up, and that's, at this point, what is most critical to us, that we would have a fleet that's in good service and ready to go with back-up.

Mr. HORN. The reason the subcommittee's interested in fire equipment is one of our first hearings was in New Orleans with the Baton Rouge chief there also, and one said to the other, "Well, gee, we haven't even thought of the fire trucks yet." And one had a pumper that was compliant and a ladder that wasn't, or vice versa, as the case may be, and I just wondered if you have that kind of relationship. Sometimes where one wasn't working at all, you could squirt the water up there, but you couldn't get up on the ladder, but you could get the ladder up, but you couldn't get the water out and so forth. So I was just curious what you found out in your equipment.

Mr. McMillan. We're confident that our equipment is going to work, but like any other organization that provides services to citizens, we're doing everything we can to have back-ups. We feel good that we do have this reserve fleet right now that can support us. What we understand about embedded systems is that maybe just a specific engine or truck out there might fail that night. If that's the case, we're ready to back it up with other equipment that's going to pump just as well.

We have sent a memorandum to our city Y2K coordinator, Mark Burton, identifying resources that the fire department will need around the Y2K millennium period, and this memorandum includes additional food, water, sanitation electrical pumps and dispatching equipment that we feel will help support us through the period.

We've also, over the past year, upgraded all of our computers. We were all MAC based, and we are now all PC based that are all Y2K compliant. All of our embedded systems, this includes over 420 pieces of equipment, are now compliant. This has been accomplished by either a letter of compliancy from the manufacturer or actual chip upgrades installed by the manufacturers.

We are working currently with the city General Services Department to identify fuel and power needs for our fire stations and apparatus.

And just giving you an example of one of the issues we wanted to deal with right up front, we go through about $50,000 worth of latex medical gloves every year. We are required when our fire fighters go out on any type of medical call to don latex gloves, and we found out earlier this year that they come from Asia. And because we don't know what the Asian nations are doing as far as Y2K preparedness, we have placed an order through an open P.O. We have annually with the vendor to buy practically $50,000, our full allotment, all at one time. We haven't figured out where we're going to warehouse it, but we're going to have all the gloves here early and not later so we don't have a problem in the next 6 months.

At this point in time, we have no information that would lead us to believe that our ability to deliver critical and essential services will be impaired by Y2K problems. There are two core service areas in the fire department in San Jose that we have identified that we are working, when we talk about our fire department contingency plan for the city of San Jose, these are the areas that we're working closely with. One's our Bureau of Field Operations. This is our first core service, and its responsibility is to mitigate emergency incidents in the community including fires, medical emergencies, hazardous material events, rescue situations and natural or terrorist caused disasters.

The emergency response system is effective when all components necessary for service delivery are readily available and functioning harmoniously. Just to give you an example, we have, in the city of San Jose, we will have 31 fire stations open during Y2K, and we will have everybody around the clock, 194 positions, assigned to those 31 fire stations. We also have an effective way of implementing call-backs systems to notify people if we need additional staff to support us during periods of need.

Our second core service is providing emergency dispatch and communication services for all our emergency response operations for the San Jose Fire Department, and the responsibility for all emergency communications systems is shared among the police department, fire department and our information technology department.

The key elements for Y2K readiness that we will be working on in the immediate future include establishing a final staffing plan and making necessary notifications to personnel impacted. We will be working closely with the police and information technology departments on the final Y2K upgrades on the city's CAD system. We will be working with our own Bureau of Field Operations staff and our Bureau of Fire Prevention staff, our fire inspectors. What we hope to do is get our fire prevention inspectors, our Haz. Mat. inspectors, our engineers on board where they can be in service and enabling during any field operations emergencies during Y2K. Finalizing contingencies in case private utilities such as water supplies, sanitary sewer systems and power supplies fail.

And one thing that we've just decided to do over the last week is we want to put together a package for all of our fire department employees on how they can be more Y2K compliant in their own residences. What we're feeling is if we could get them to be a little less apprehensive during any kind of emergency over Y2K, they might be more apt to be available to come down to the city of San Jose and help us in need.

In summary, the San Jose Fire Department has prepared this plan assuming a worst-case scenario, similar to how we may have to operate in a major disaster. If all or some technology systems fail, we will be prepared to operate in a manual mode. As in any situation where a high demand is placed on our resources, and our capabilities and effectiveness may be limited by a number of external forces, our goal is to provide the highest level of emergency services possible. To do this will likely result in prioritization of emergency calls in order to mitigate the most serious incidents.

Thank you, sir.

[The prepared statement of Mr. McMillan follows:]

CITY OF
SAN JOSE
CAPITAL OF SILICON VALLEY

Congress of the United States
House of Representatives

Year 2000 Departmental Plan & Contingency Strategies
Saturday, August 14, 1999
San Jose City Hall

Statement of John A. McMillan, Deputy Chief
Director of the Bureau of Support Services
City of San Jose Fire Department

MISSSION STATEMENT:

The mission of the Fire Department is to serve the community by minimizing losses from fire and other hazards through courtesy and service with pride.

The San Jose Fire Department has evaluated Mission Critical and Mission Essential Core Services for Y2K readiness. As of this submission, the Department is confident that we will be able to fulfill our mission. Fire Department staff continues to evaluate mission-related systems and process and is developing contingency methods of service delivery in the event that unforeseen Y2K problems should occur. We are specifically focusing on and making decisions in the following areas:

- Upgrading all 50 of our Emergency Medical Defibrillators to Y2K compliance, which is now complete.

- We have placed a hold on releasing all surplus fire apparatus. This was a critical decision since so many of our front line apparatus are new in the last five (5) years and have numerous embedded systems. This decision has allowed us to hold fifthteen (15) fire engines in reserve.

- We have sent a memorandum to Mark Burton, our City Y2K coordinator, that identifies resources that we will need for at least three (3) days around Y2K. They include food, water, sanitation, portable electrical pumps and portable dispatch units.

- We have upgraded all of our computers from MAC to Y2K compliant PC's in the past year. Essential software that allows an emergency response operation are also upgraded to Y2K compliancy.

- All of our embedded systems, including over 420 pieces of equipment are now compliant. This has been accomplished by either a letter of compliancy from the manufacturer or actual chip upgrades installed by the manufacturer.

- We are working with the City's General Services Department to identify fuel and power needs for our fire stations and apparatus.

- We have placed a full year's order of latex medical gloves instead of incremental orders throughout the fiscal year. Our understanding is latex medical gloves come from Asia and we don't know what preparedness other countries have made for Y2K. Latex medical gloves are essential to our delivery of service because our personnel are required to wear them on all medical calls.

At this point in time, we have no information that would lead us to believe that our ability to deliver critical and essential services will be impaired by Y2K problems.

We have two (2) areas we have identified as our core services that are essential and they include:

I. ***BUREAU OF FIELD OPERATION***

The First core service is to mitigate emergency incidents in the community including fires, medical emergencies, hazardous materials events; rescue situations and natural or terrorist caused disasters.

The emergency response system is effective when all components necessary for service delivery are readily available and functioning harmoniously.

Emergency Response Staffing

- 31 Fire Stations
- Normal Emergency response staffing is 190 positions every day (194 effective 10-1-99).
- Extraordinary staffing needs are addressed by a call back system.

2. Communications Division

Our second core service is providing emergency dispatch and communication services for emergency response operations of the San Jose Fire Department.

Responsibility for all Emergency Communications Systems is shared among Police, Fire and Information Technology Departments.

The key elements for Y2K readiness that we will be working on in the immediate future include:

- Establishing final staffing plans and making necessary notifications to personnel impacted.

- Working closely with the Police and Information Technology Departments on the final Y2K upgrade to the City's CAD System.

- The Bureau of Field Operations (BFO) and Bureau of Fire Prevention (BFP) staff will meet specifically to discuss how BFP personnel can be service enabling to emergency operation.

- Finalizing contingencies in case private utilities such as water supply, sanitary sewer systems and power supply fail.

- Provide information to all Fire Department employees on how to be Y2K compliant at home so they are less apprehensive and more apt to be available to the City needs during the Y2K critical hours

SUMMARY:
We have prepared this plan assuming a worst case scenario; similar to how we may have to operate in a major disaster. If all or some technology systems fail, we will be prepared to operate in a manual mode. As in any situation where a high demand is placed on our resources, and our capabilities and effectiveness may be limited by a number of external forces, our goal is to provide the highest level of emergency services possible. To do this will likely result in the prioritization of emergency calls in order to mitigate the most serious incidents.

Mr. HORN. Thank you. That's most useful, and I look forward to the details on that.

Let me ask our power suppliers, Pacific Gas and Electric, Silicon Valley Power. There are about 3,200 independent electric utilities, I think, in the United States, and there's about 80 percent of the Nation's power generation comes from 250 investor owned public utilities. We all know it takes a high degree of automation, and you've mentioned that, to operate our country's national power grid.

But just to get it in the record at this point in terms of the lights being able to stay on, the assembly lines being able to run, I guess I would ask what is being done to keep home owners and businesses informed about potential failures in their energy management system, or are you just assuming with the general education, which has been very good, that you've let out to your customers, either in bill or special sessions or whatever, I'm just curious, are people, are some of your customers worried that there might be an interruption, and if so, what? Is there a back-up to that, either within the grid or if we talk about hospitals and emergency rooms, some of them say we've got 72 hours of power based on diesel generators and all that. I don't know. Is that really useful? I mean, it will work for awhile, but suppose we have 3 or 4 days out, and they can't get the fuel and they're sort of just behind the eight ball? So I'd just be curious what your thoughts are on this.

Mr. GARTH HALL. From PG&E's point of view, I would say that our customer base has an uneven, on average a modest level of interest and concern about it. Our website, which I mentioned earlier, receives about 9,000 hits a year in the section that deals with Y2K—sorry, 9,000 a month. That's the current rate of hits, which given our service territory is not very large.

We have, of course, bill inserts that have gone out to inform the public, the customers, as to our readiness and direct them to normal preparedness, that I think Dr. Winslow suggested, will be appropriate for this time of the year as we're going into the winter storms, and for earthquakes. That's a good opportunity to brush up on the type of items that you would typically want to have in store for these types of emergencies. Y2K is an opportunity for folks to think about preparedness for general emergencies like these.

But in addition to that, I did mention that we have had, for all the customer groups that have expressed an interest, we've had face-to-face meetings with them and presentations to point where I think we've seen them tail off in that type of demand for a meeting, although we're ready at any time to meet with folks who are interested.

We plan additional inserts into the bills that go out to our customers to just keep them updated. We think that there is going to probably be some level of increased interest as we approach the end of the year, and we will definitely be updating our website to provide any current status information. We think that our call centers which people, customers, well know, which has a 1–800 number, will be very, very capable and well prepared to answer any questions that people have if they want to call in with any need for information. During the New Year transition timeframe we expect that the press will be very interested in what's going on, and we're preparing ways in which we can keep them informed in real time as to what's going on.

Those are some of the steps we've taken. We'll probably do additional things as we go through.

Mr. HORN. Ms. Lopez, do you want to add anything to that?

Ms. LOPEZ. Actually, it's pretty much the same thing as we are doing. I think we have one advantage in being a small, local municipal service. We have many of our citizens that are concerned actually drop in and talk to us. But we do have, which we have sponsored and we have two more scheduled to be sponsored, meetings within the communities themselves, at the library, one at a local park. Plus, as I said, we have done with all the commercial and industrial customers, had several meetings, and we will have more.

I think it's not a matter of awareness. I am, I guess, amazed somewhat at the level of concern and that the number of individuals seems to be very small that have concerns, but of those that are concerned or even partially aware, electricity does seem to be their No. 1 priority.

As to your question regarding generation, we are encouraging all of our households, have back-up fuel as a concern. We have allocated within the city areas where we can have extra fuel that could be delivered if it were needed. We don't believe it will be, but we have made preparations for that.

We also have—we don't have within our city the ability to completely supply generation for all of our needs. We must rely on ol' PG&E for that. We do have some measures available, particularly for emergency type facilities and situations that we think will be adequate if anyone would need them.

Mr. HORN. I was going to ask you on the point you just raised, which was, PG&E is the source for what percentage of your power? You buy it from them at a good deal, is that it?

Ms. LOPEZ. Yes, sir. Probably, not probably, definitely the majority of our power, we would be unable to sustain service, other than very minimally with our in-city generation.

Mr. HORN. What percent of your total power is provided by PG&E?

Ms. LOPEZ. I think it's somewhere around 95 percent.

Mr. HORN. 95?

Ms. LOPEZ. 95 percent.

Mr. HORN. And you generate the last 5 percent how?

Ms. LOPEZ. Yes, sir. Well, we don't normally generate it. We normally use 100 percent from without, but we do have abilities within our city for some generation.

Mr. HORN. What is that? Your own generators?

Ms. LOPEZ. Yes, sir. Our own power.

Mr. HORN. Fuel operated?

Ms. LOPEZ. Yes, sir.

Mr. HORN. Now, if PG&E is in a caught, how many of those contracts do you have out that you supply from PG&E, and if you were in a squeeze, do you cancel those contracts or can they count on it?

Ms. LOPEZ. Would they cancel? We wouldn't cancel those contracts.

Mr. HORN. Well, would PG&E cancel them, I guess what I'm asking Mr. Hall is, in other words, if you're put with a major disaster on your hands, do you just cancel the contracts for small power companies and feed your more prominent customers or areas that might not have small companies?

Mr. GARTH HALL. That's not the approach at all. Let me just mention in a sound byte that the electric restructuring that has been initiated across the Federal terrain has had a very, very big impact over the last 2, 3 years in California. Right now, the power that is delivered to Santa Clara and many other very language cities and customers, often they have very, very little now comes from PG&E. They contract for supply from independent providers. I think you mentioned that in your prior question, of which there are many thousands of individual generators now. That is the bulk source of most of the power.

Our primary responsibility in the electric side is in the delivery, and that is the area where, in fact, cities like Santa Clara and many others do depend on us very much for our reliability, we've focussed very much on that.

Let me just mention one additional thing that might be reassuring, that the Western Systems Coordinating Council, which is a part of the North American Reliability Council in dealing with the western systems reliability, have announced plans over the New Year transition, which would be several hours before midnight hour and several hours afterwards, whereby all of the power plants within that jurisdiction will have additional reserves. The way they will do that is bring additional power plants online and back all of those that are online down a bit. So that if there are, heaven forbid, some power plant failures due to microchip problems or whatever, that they will have additional reserves to instantly step up and provide additional power.

In addition to that, the demands, I think, even Santa Clara would receive from the Pacific Northwest, by the entire Northwest, those vulnerabilities, if there are any, will be reduced by reduced schedules across the entire so that we are more self-sufficient for that vulnerable period, just with the normal state. So I think very prudent measures have been made to avoid the types of failures that we have contemplated nationally amongst power plants.

Finally, I will say that since we're an owner of a very large independent power producer with more than 25 power plants across the United States, I have personally overseen their Y2K compliance efforts they have been through, and I believe this is fairly typical, as stringent a Y2K program as anything that the utility has done. So I think their readiness is equally as strong as I'm representing for the utility.

Mr. HORN. Mr. Willemssen has joined us at the table. Let me ask you what we didn't ask you yesterday just for this record. Santa Clara is a very urbanized county and very complex, and great demands on power. Get across the Pajaro River into San Benito County, you have people, farms stretched out over, maybe a mile apart, half mile apart, 10 miles apart.

What do you find in terms of the rural part of the PG&E jurisdiction as you go up, let's say, Sierra County and Plumas and all the way to the Oregon border. Are you finding different reactions to the year 2000 in the rural areas where they don't have the money to sort of adapt to whatever systems they're using? What's been the experience?

Mr. GARTH HALL. We have found it to be fairly uneven. Yesterday we had a representative from, I believe, Siskiyou County, and I think that was interesting, because they demonstrated a very high level of awareness for a county with a relatively small population.

That is uneven in our experience. Wherever there is a need or interest, we have been responsive and tried to provide the information. As I mentioned, most of them, in fact, all of the them, in their emergency services at the police level and at the Office of Emergency Services level, are very aware of the distribution emergency centers that we have uniformly positioned across our service territory, and are well versed in interacting with those centers at times of emergencies.

So from the staff who deal with emergency, from their point of view, we think we have excellent contact. From the general public point of view, again, fairly uneven.

Mr. HORN. Interesting.

Do you want to add anything, Ms. Lopez, based on your experience?

Ms. LOPEZ. No, sir.

Mr. HORN. Let me ask the chief and Dr. Winslow and Mr. McMillan, the deputy fire chief, how ready are we on the 911 systems that typically rely on older telecommunications and computer equipment? Do you feel that if there's a flood of these calls because people are just upset or whatever; they don't know; it's like having an eclipse nobody told us about; it's awful dark outside. We'll phone you. So what's your reaction to that system?

Mr. LANSDOWNE. Mr. Chairman, Bill Lansdowne from the police department. We have planned for this. We will have additional persons who will be on standby and actively working the phones. So we will easily be able to handle any anticipated increase in the number of calls.

We just recently upgraded our 911 system. It's state-of-the-art. It's compliant. I don't think that we're going to have any trouble at all handling the 911 increase in calls. I'm very proud to state that we currently handle our pickup of 911 calls within 2.2 seconds, which is one of the fastest in the Nation of any city this size. Of course we handle 900,000 people here.

Mr. HORN. On the frequencies that different police forces have within Santa Clara County, I'm curious, is there a united frequency here? I went through this in L.A. County several years ago, and we have 81 cities in that county and 10 million people. We've got the Sheriff. We've got the University of California, California State University, State Police, all different little jurisdictions, if you will.

Is there any problem here that you lack the frequencies that you need to communicate to smaller groups within various cities and police forces?

Mr. LANSDOWNE. None of our systems are compatible right now with the State agencies, Highway Patrol and the local jurisdictions, Santa Clara and San Jose, and the county jurisdiction. But the communication systems are linked, and that will be the way that we will have to communicate from department to department, if we are required to do a Mutual Aid System. I think we are very fortunate in the State of California that we have a very comprehensive Mutual Aid System, and all of the agencies, the sheriff, the local agencies in the Bay Area regions are prepared to provide whatever mutual aid which will be requested from us, and we have that system in place.

Mr. HORN. You could provide that in terms of triggering it by what? Telephone? Radio frequency?

Mr. LANSDOWNE. The system triggering is calling the sheriff who is the natural disaster person within the county, and then they would trigger at the level they need. My understanding and maybe the panel can add to that, is that the State will be up and ready to put that system in place and operate it during the New Year's.

Mr. HORN. Now, will that be a permanent system or is that just for potential emergencies?

Mr. LANSDOWNE. It's for potential emergencies, natural disasters of which this State has a lot of experience.

Mr. HORN. That's for sure. We have the biggest number of disasters in the Nation. When you look at it from the Mississippi, they have floods. We outdo them with earthquakes. I think the Loma Prieta is still the most expensive Federal investment isn't it?

Ms. WINSLOW. Northridge.

Mr. HORN. Northridge is still? I know there's a few things not settled yet on hospitals and whatnot, but so what's that? About 16 billion?

Ms. WINSLOW. That's the FEMA cost. If you look at the insurance loss on top of that, it's a much bigger number.

I'd just like to clarify on the Mutual Aid System. The Mutual Aid System has been in place since the 1950's, and it's maintained at all levels of law enforcement on one chain and fire on the other chain. At the top of the chain is the State Office of Emergency Services. They will be opening the State Operations Center and the Regional Operations Centers in each regional office, which is Sacramento, Oakland and in your area it's at the Los Alamitos former reserve center. Those will be open December 30th, and they will open through the 2nd.

Mr. HORN. Now, are the National Guard and the Army Reserve also tied into these? What sort of relationship would you have there? Let's say you had a riot.

Ms. WINSLOW. The National Guard is called out by the Governor on a request from the local chief of police, and the military is only activated under very unique circumstances where the Governor and the President concur.

Mr. HORN. All right.

Mr. LANSDOWNE. I would like to say, Mr. Chairman, that they are on standby, and they will have people in the operation of Emergency Services Centers during a 72-hour period. They could be activated at a moment's notice with a call to the Governor of the State of California.

Mr. HORN. And those frequencies exist with the Federal portion like the Reserve and the National Guard, so there is rapid communication there other than telephone? Let's say with all due respect to Pacific Bell, but.

Mr. LANSDOWNE. Yes, sir. Those systems are in place. We can have Federal assistance very quickly.

Mr. HORN. Mr. Willemssen, what do you have to add to this panel? I saw you taking a lot of notes.

Mr. WILLEMSSEN. I just thought that you, Mr. Chairman, might also get some value out of hearing in the Y2K emergency services area what kind of assistance and interaction that the individuals here received from FEMA and any kind of communications they received recently from the newly formed Information Coordination Center headed by General Kind. There are a lot of activities under way that will involve not only the FEMA regional offices, but all the States and localities, and I think it would be of interest to hear what kind of communications have occurred at this point.

Mr. HORN. Yeah. Well, don't all rush to the microphone now.

Ms. WINSLOW. I guess I'll just have to deal with this one because my office deals with people the most. I don't think there's really a politically correct way to say this. We haven't heard anything from anybody.

Mr. HORN. In other words, there's a lot of work to be done between now and December.

Ms. WINSLOW. I only know what I read in the newspaper.

Mr. HORN. I see. So how's the system supposed to work? Is it supposed to work through the FEMA regional office or directly out of Washington or what?

Ms. WINSLOW. No. In California we have a structure called the Standardized Emergency Management System, which establishes the way that we relate to each other. So the cities together with the county are called an Operational Area, and we're the Santa Clara County Operational Area. We're part of the Coastal Region which goes from the Oregon border to the southern border of Monterey County, and from the ocean to the coastal foothills, and along that strip, we are joined through that office in Oakland, which serves as a head of that. We have periodic meetings, four times a year, with the Coastal Region Leadership. Generally information that we get from FEMA comes through the State through the Coastal Region to us at those meetings.

Mr. HORN. And you're meeting twice a year?

Ms. WINSLOW. No. Four times.

Mr. HORN. Four times a year.

Ms. WINSLOW. In fact, there's a meeting at the end of this month. So perhaps that's the time. This is a relatively new effort on FEMA's part. It may be that at the August meeting they'll present the information, but to date we haven't received anything that I'm aware of.

Mr. HORN. OK. Mr. Willemssen.

Mr. WILLEMSSEN. I would just add that the newly formed ICC and FEMA are planning a major exercise September 9th. It's supposed to involve the unifying State contacts. The plan is that each of the unified State contacts is supposed to supply information upwards to individual FEMA Regional Offices, which will then be supplied upwards to the national level. You may be hearing more about that shortly.

Mr. HORN. September, 9th, 1999, is also the nationwide power grid drill; is that correct? Is that tied in with the same thing by FEMA?

Mr. WILLEMSSEN. No. Those are predominantly separate efforts, although John Koskinen will obviously be monitoring both simultaneously.

Mr. HORN. That's the representative to the President, the executive branch.

Any other questions we have? Any other thoughts any of you have after having listened to three panels including yourself?

Well, if you have them, we'll be glad to put them in. We keep the record open for a week or so, and we'll put them in at this point. And we have several questions from the audience, and we will be writing to the relevant panel members, and we'll put them in at the appropriate place in the record. So without objection that will be done.

I just want to say as one that was brought up in this area, I appreciate very much all of the fine work that these three panels have done. I think that's been very helpful that you sort of restore our confidence in the degree to which local government, the county, the particular groups whether it be hospitals that we had on the panel of yesterday, police today, and all the rest of it, that people are cooperating and are working together, and that is, I think, impressive.

Let me just thank the staff that have worked on this particular hearing. J. Russell George, staff director. There we are, down, front row seat. Did you pay a high ticket price for that? He's our chief counsel also.

To my left and your right is Patricia Jones. Patricia is with us as a fellow, congressional fellow of the American Political Science Association.

And Bonnie Heald, our communications director, is also in the front row, a professional staff member.

And Mr. Ahlswede is not here. He's already ahead of us in Portland, and he is the clerk.

And then Seann Kalagher, an intern, is around here somewhere. There you are. Good to see you.

And then from Mr. Campbell's staff, Casey Beyer is the chief of staff, and we thank him for his help.

And Sally Wilson is our court reporter, and we thank you very much for going through 3 hours of this yourself.

And with that we wish you well, and we recess this meeting.

[Whereupon, at 12:50 p.m., the subcommittee was recessed, subject to the call of the Chair.]

THE YEAR 2000 COMPUTER PROBLEM: LESSONS LEARNED FROM STATE AND LOCAL EXPERIENCES

TUESDAY, AUGUST 17, 1999

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY,
COMMITTEE ON GOVERNMENT REFORM,
Seattle, WA.

The subcommittee met, pursuant to notice, at 9 a.m., at the Henry M. Jackson Federal Building, 915 Second Avenue, Seattle, WA, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representative Horn.

Also present: Representatives McDermott and Dunn.

Staff present: J. Russell George, staff director and chief counsel; Matthew Ryan, senior policy director; Patricia Jones, congressional fellow; Chip Ahlswede, staff assistant; and Grant Newman, clerk.

Mr. HORN. Good morning. I'm Steve Horn, chairman of the House Subcommittee on Government Management, Information, and Technology. This hearing, which recessed in California on these issues, will now come to order.

I particularly welcome and thank my two colleagues from the Seattle area, Congresswoman Jennifer Dunn and Congressman Jim McDermott. We're delighted to have them with us, and they will participate as full members in terms of asking questions, opening statements, whatever. We will treat them with great courtesy because they are major leaders within the House of Representatives and their respective parties.

And we are here to discuss a topic of worldwide interest, the so-called year 2000 computer problem, also known as Y2K, and commonly referred to as the millennium bug. The year 2000 technology challenge affects just about every aspect of Federal, State and local government operations. Furthermore, it affects private sector organizations and could impact the lives of most individuals. From Social Security to utilities to local emergency management, the year 2000 computer bug has certainly been a huge and large management and technological challenge for all of us. No single organization, city, State, or even country, can solve the year 2000 problem alone.

We have 136 days before January 1, 2000. There is only one certainty with the year 2000 problem: that date is certain, and no one is certain as to what will exactly happen on that day.

Our goal is to ensure that citizens' vital services are maintained. There are many unknowns, including international readiness.

The problem, of course, dates back to the mid-1960's, when programmers, seeking to conserve limited computer storage capacity and memory, began designating the year in two digits rather than four. In other words, the year 1967 became '67 in the computer. And they knew at that time that when you got to the year 2000, it would come up 1900, and the computer wouldn't know if it was 2000 or 1900. The computer would be confused. And that's what we have been working on for the last 4 or 5 years.

And they said at the time, "Well, we won't have to worry. After all, we're Americans, and technology will solve this."

Well, it won't. It hasn't. And just hard work and going through those codes and everything else is what it has taken to prepare for the January 1, 2000 situation.

Our subcommittee has the jurisdiction over the executive branch agency and Cabinet departments on matters of economy, efficiency, and effectiveness. We held our first hearing on the problem in the spring of 1996. Since that time, we've held over 30 hearings and issued eight report cards to monitor the status of the Federal Government's year 2000 computer solution.

You will hear today from the State of Washington that they have 423 mission-critical, or essential, computer systems. The Federal Aviation Administration, one Federal agency, has roughly the exact same number.

This is a situation that relates to interoperability between the Federal Government, the State government, the county governments and the local and city governments.

Current estimates show that the Federal Government will spend nearly $9 billion to fix its computer systems. I've often said the figure will probably reach about $10 billion by the end of the December 31st calendar year.

And we have also worked on looking at business continuity and contingency plans as well as Federal. We work with Mrs. Morella's Committee on Technology of the House Science Committee that relates to Mr. Bennett's Senate committee. The Senate didn't start on this until 2 or 3 years after we did, and they started in roughly February 1998. The administration started with putting a full-time person on the job in April 1998.

These plans that we have looked at on a quarterly basis provide critical insurance in the event of unforeseen problems.

Recently, the President's Office of Management and Budget identified 43 essential Federal programs, such as Social Security, Medicare, the Nation's air traffic control system, the weather system. Each day, these programs provide critical services to millions of Americans. Of these 43 programs, 10 are federally funded, State-run programs, such as Medicaid, food stamps, unemployment insurance, and child support enforcement. Several of these State-run programs are not scheduled to be ready for the year 2000 until December, leaving little, if any, time to fix unforeseen problems.

Data exchanges and interdependencies exist at all levels of government and throughout the private sector. A single failure in the chain of information could have severe repercussions.

For example, the U.S.' Social Security program has been ahead of everybody else on its own initiative. No President ever had to tell them what to do. They decided in 1989 to do it, and they were the first Federal agency to have 100 percent compliance.

The Social Security Administration maintains data containing pertinent Social Security payment information for eligible citizens. When payments are made, the Social Security Administration sends payment data to the Department of the Treasury's Financial Management Service. Now, that was way behind this year. They are now coming up to snuff. This service cuts the Federal checks, which are generally electronically deposited directly into the person's bank account at a local financial institution.

Three organizations move and manipulate data to make these payments happen; each uses a network of computers. If a payment is mailed to the individual's home, the U.S. Postal Service plays a key role. And most of the Federal agencies told us that their contingency was the U.S. Postal Service.

We then held a hearing with the Postal Service, and it turns out they had no contingency plan. So there are problems there.

The bottom line is, if any one of these entities fails, from the Federal Government to the local bank or with the Postal Service, the checks going to the home of a deserving individual simply might not ever get there.

Now, multiply this situation by the 43 to 50 million different checks Social Security makes out in 1 month and you can appreciate the magnitude of just one aspect of the year 2000 issue.

Fortunately, the Social Security Administration has been working on the problem, as I said, since 1989, and it's 100 percent compliant.

But for computers to work, we need energy, electric power, whether it be hydro, nuclear, wind, whatever, and that is essential. And we will hear today from the local utilities. We've done that in every city we've been in, which are roughly about 20 city and State visits.

One of the most essential questions concerning the year 2000 challenge is, "Will the lights stay on?" Without electricity, the assembly lines of one sort or another simply stop, and people would be let off after a certain period if there was a drastic blackout that went beyond just a few days, and our modern society might seem to be in the Stone Age when there is no power. We look forward to hearing today from the Bonneville Power Administration, Seattle City Light, and Puget Sound Energy to answer that question.

From a personal standpoint, I realize that when confronted with a personal emergency—and you do, too—I can call 911 for assistance, and we should feel confident that that phone will be answered promptly and that a competent authority will respond rapidly. So we will be hearing from public safety individuals, as we do at every city hearing.

Year 2000 computer problems present other potentially serious threats at local levels, from the potential interruption of a city's call for fire or police assistance to delays in a State's ability to request emergency or disaster assistance from the Federal Government.

One thing is certain: there are only 136 days until January 1st, and the clock is ticking. Accordingly, the testimony we receive today will help our understanding and the community's understanding of the full extent of the year 2000 problems in the State of Washington.

Today, we have three knowledgeable panels to provide a picture of year 2000 readiness in both the public and private sectors, and I welcome all of our witnesses. But first, I'd like to call, in terms of seniority, which is the way we resolve these conflicts in the House of Representatives, the gentleman from Seattle and State of Washington, Mr. McDermott, for any opening statement he might wish to make.

[The prepared statement of Hon. Stephen Horn follows:]

DAN BURTON INDIANA
CHAIRMAN

BENJAMIN A GILMAN, NEW YORK
CONSTANCE A MORELLA MARYLAND
CHRISTOPHER SHAYS CONNECTICUT
ILEANA ROS-LEHTINEN FLORIDA
JOHN M McHUGH, NEW YORK
STEPHEN HORN CALIFORNIA
JOHN L MICA FLORIDA
'HOMAS M DAVIS III, VIRGINIA
AVID M McINTOSH INDIANA
MARK E SOUDER, INDIANA
JOE SCARBOROUGH FLORIDA
STEVEN C LATOURETTE, OHIO
MARSHALL "MARK" SANFORD, SOUTH CAROLINA
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
ASA HUTCHINSON, ARKANSAS
LEE TERRY, NEBRASKA
JUDY BIGGERT, ILLINOIS
GREG WALDEN, OREGON
DOUG OSE, CALIFORNIA
PAUL RYAN, WISCONSIN
HELEN CHENOWETH, IDAHO
DAVID VITTER, LOUISIANA

ONE HUNDRED SIXTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
MINORITY (202) 225–5051
TTY (202) 225–6852

HENRY A WAXMAN, CALIFORNIA
RANKING MINORITY MEMBER

TOM LANTOS CALIFORNIA
ROBERT E WISE JR., WEST VIRGINIA
MAJOR R OWENS NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E KANJORSKI PENNSYLVANIA
PATSY T MINK HAWAII
CAROLYN B MALONEY NEW YORK
ELEANOR HOLMES NORTON
DISTRICT OF COLUMBIA
CHAKA FATTAH PENNSYLVANIA
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J KUCINICH, OHIO
ROD R BLAGOJEVICH, ILLINOIS
DANNY K DAVIS, ILLINOIS
JOHN F TIERNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H ALLEN MAINE
HAROLD E FORD JR TENNESSEE
JANICE D SCHAKOWSKY, ILLINOIS

BERNARD SANDERS, VERMONT
INDEPENDENT

"Oversight of the Year 2000 Problem: Lessons to Be Learned from State and Local Experiences"
Opening Statement of Chairman Stephen Horn (R-CA)
Subcommittee on Government Management, Information and Technology
August 17, 1999
Seattle, Washington

This hearing of the House Subcommittee on Government Management, Information, and Technology will come to order. I would like to welcome and thank Congresswoman Jennifer Dunn and Congressman Jim McDermott for being such gracious hosts as the subcommittee meets today in Seattle. We are here today to discuss a topic of great interest worldwide: the Year 2000 computer problem, commonly referred to as the "millennium bug."

The Year 2000 technology challenge affects just about every aspect of Federal, State, and local government operations. Furthermore, it affects private sector organizations and could impact the lives of most individuals. From Social Security to utilities to local emergency management, the Year 2000 computer bug has certainly been a large management and technological challenge for all of us. No single organization, city, State or even country can solve the Year 2000 problem alone.

There is only one certainty with the Year 2000 problem: no one is certain what exactly will happen and when. Our goal is to ensure that citizens' vital services are maintained. There are many unknowns, including international readiness.

The problem, of course, dates back to the mid-1960s when programmers, seeking to conserve limited computer storage capacity, began designating the year in two digits rather than four. The year 1967, for example, simply appeared as '67.' Regardless, now we all must deal with it.

More than three years ago, our subcommittee held the first Congressional hearing on the Year 2000 problem. Since that time, we have held over 30 hearings and issued 8 "report cards" to monitor the status of the Federal Government's Year 2000 computer solutions. We will hear today that the State of Washington has 423 mission-critical, or essential, computer systems. The Federal Aviation Administration, one Federal agency, has roughly the exact same number.

Current estimates show that the Federal Government will spend nearly 9 billion dollars to fix its computer systems. I have often said that figure will easily reach 10 billion dollars. These funds have been spent to fix Year 2000 problems and to develop comprehensive business continuity and contingency plans. These plans provide critical insurance in the event of unforeseen problems.

Recently, the President's Office of Management and Budget identified 43 essential Federal programs such as Social Security, Medicare, and the nation's Air Traffic Control system. Each day, these programs provide critical services to millions of Americans. Of these 43 programs, 10 are Federally funded, State run programs including Medicaid, Food Stamps, Unemployment Insurance, and Child Support Enforcement. Several of these State run programs are not scheduled to be ready for the Year 2000 until December, leaving little, if any, time to fix unforeseen problems.

Data exchanges and interdependencies exist at all levels of government and throughout the private sector. A single failure in the chain of information could have severe repercussions.

For example, let me briefly illustrate how the United States' Social Security program uses computers. The Social Security Administration maintains data containing pertinent Social Security payment information for eligible citizens. When payments are made, the Social Security Administration sends payment data to the Department of the Treasury's Financial Management Service. This Service then "cuts the Federal check," which is then electronically deposited directly into a person's bank account at a local financial institution. Three organizations move and manipulate data to make these payments; each uses its own network of computers. If a payment is mailed to an individual's home, the United States Postal Service then plays a key role.

The bottom line is: If any one of these entities fails, from the Federal Government to the local bank or Postal Service, a deserving individual will not receive the payment. Now multiply this situation by the millions of people that receive Social Security benefits and you can appreciate the magnitude of just one aspect of the Year 2000 issue. Fortunately, the Social Security Administration has been working on this problem for 10 years and is in good shape.

But, for computers to work, we need power. One of the most essential questions concerning the Year 2000 challenge is, "will the lights stay on?" Without electricity, our modern society would be relegated back to the proverbial "Stone Age". We look forward to hearing today from the Bonneville Power Administration, Seattle City Light, and Puget Sound Energy to answer that question.

From a personal standpoint, I realize that when confronted with a personal emergency, I can call 911 for assistance and feel confident that the phone will be answered promptly and that a competent authority will respond rapidly. Year 2000 computer problems present other potentially serious threats at local levels, from the potential interruption of a citizen's call for fire or police assistance to delays in a State's ability to request emergency or disaster assistance from the Federal Government.

One thing is for sure, there are only 136 days until January 1, 2000, and the clock is ticking. Accordingly, the testimony we receive today will help our understanding of the full extent of the Year 2000 computer problem.

Today we have assimilated three wonderful panels to provide a picture of Year 2000 readiness in both the public and private sectors.

I welcome all of today's witnesses and look forward to their testimony.

For more information on the Subcommittee's work, please visit our website:

www.house.gov/reform/gmit

Mr. McDERMOTT. Thank you very much. Welcome to Mr. Horn, the good representative from Long Beach, where I spent a couple of years back in 1968 to 1970 during the Vietnam War. So I know a little about your district, and it's good to have you here.

I really do not have an opening statement because I really came to hear what's going on. We've had lots of hoopla and we've passed bills to get rid of liability for Y2K and all these sorts of things in Congress, but I've not yet heard in my own community, in an organized way, where we stand. So I'm very eager to hear what we have today, and I thank you for coming to Seattle to have this hearing.

Mr. HORN. I'm delighted to have my classmate from the elections of 1992, Jennifer Dunn, who has been a real leader in her party and an excellent representative from her area, here.

And as you know, Washington is one of the most progressive States in the country. And with your great port, The Boeing Aircraft Co., which I also have a part of—in other words, Douglas Aircraft, which is now Boeing, is in my district—so we have a lot in common. And Norm Dicks and I won't have to argue with each other.

Ms. DUNN. That's a relief.

Steve, we're so happy you're here with us today. And it's certainly the pleasure of all of us, those joining us in the audience, to welcome you on what's something like the 20th hearing on Y2K problems that may be in existence, and success stories that we know certainly do exist around this Nation.

I want to thank, too, Bruce Chapman of the Discovery Institute. Bruce, perhaps you could stand at the back of the audience. Bruce has been a great facilitator of this meeting today, as we invited Congressman Horn to join us in Seattle. And Bruce Chapman will host him at lunch today so that we can hear a little bit more about what's happening behind the scenes on Y2K.

I also want to mention a couple of the folks in the audience that are particularly important to me. We have three members of my Youth Advisory Council sitting in the audience today, and they came because they are interested in what's going on in this Nation. And they are 3 among 30 young people who advise me on issues across the board and give us a point of view that we often do not receive, which is that of young people who are operating in the real world out there.

So I'd like to ask Mary Basinger and Nicole Leonce and Omar Hakim to stand. Mary is from Green River Community College, and Nicole goes to Kentwood High School, and Omar is a student at Newport High School. And we're delighted that you could be here today with us.

As most of us would agree, the importance of preparation and readiness for year 2000 simply cannot be understated. So much of Americans' daily lives revolve around computer transactions and digital events that most people probably are not even aware of.

Now, I'm an old systems engineer with the IBM Co. during the 1960's, and that was my job out of Stanford University. And I see you're a graduate, too. But I came home to Seattle and did a lot of work, and I remember the long hours of turning people's accounting systems into computer programs, and then the even longer hours of debugging those programs.

And so my particular concern is how the testing of the programs that have been started and that we'll hear about today, how the testing is going and whether we will be reliably sure that by the time we have that turnover, those tests will result in successful systems.

It's up to all of us to be sure that when the clock turns to midnight on December 31st of this year, water, power, and emergency services are on line and are working for the residents of our State. So I, too, look forward to hearing the testimony of the folks who have joined us here today.

We also need to know about the interactions among the companies and the agencies we'll hear from today, and the Federal agencies that Jim McDermott and I actually oversee, since we're members of the Oversight Subcommittee of the Ways and Means Committee in the U.S. Congress.

Now, we have participated in a large number of oversight hearings on the readiness of Federal agencies under the jurisdiction of the Ways and Means Committee, like the Social Security Administration. And as Congressman Horn says, fortunately that administration is well ready to get those checks in the mail, and that's something we're very concerned with.

The IRS is another agency under our jurisdiction, not in quite such good shape, unfortunately, but doing better under a great manager who has taken over the IRS.

Medicare and the U.S. Customs Service are also under our jurisdiction, so we have heard hearings from those agencies.

Now, they are all in different stages of readiness for Y2K, and they all have comprehensive plans to fix the problem ahead of time and to deal with emergencies should those arise.

As the clock winds down on the millennium, it's our job to continue to oversee these efforts. And the fact that Congressman Horn has seen fit to come into the Seattle area and offer an opportunity for us to hear from the different agencies should be certainly congratulated, and I think it will do us all a lot of good to hear what's going on in the Seattle community and the State of Washington today.

I want to thank you particularly, Congressman Horn, for coming here and doing this for us.

Mr. HORN. Thank you very much, Representative Dunn.

Let me just explain how this subcommittee functions. We'll have three panels. Each one will probably take about an hour. The individuals in each panel will be as they are shown in the agenda. We simply go down the line.

We have their written papers. They automatically become part of the record when we introduce them. We'd like them to summarize those remarks and presentation in about 5 minutes. And counsel here will sort of keep track. And the reason for that is we'd like a dialog within the panel and between the subcommittee and my two colleagues from Washington and the individuals here who think we get at the questions and the understanding best that way. And we thank you very much for the very fine papers you've filed with us.

We will also, as an investigating committee of the House, swear in all panels. If you have staff back of you that supports you, please, we'll have them stand with you—the clerk will note who has affirmed the oath—and that permits the testimony to be taken.

So if the first panel would stand and raise your right hands. And anybody in your support staff, please have them stand. I only do one baptism. We have five at the witness table, two behind.

[Witnesses sworn.]

Mr. HORN. I take it the two back there look like they also affirm. So the clerk will note that, and we'll proceed. Now, our lead witness in every panel we have across the Nation is a representative of the General Accounting Office. The General Accounting Office was established by law in 1921, when the President was also given a Bureau of the Budget, and the Congress, which is the legislative branch. And it's the GAO, the General Accounting Office, that works for us, and they work on both fiscal matters and programmatic matters.

And Joel Willemssen, who will be the first witness here, the Director of Civil Agencies Information Systems, has been in every one of our panels.

Now, we had several going last week. He happened to fly to Washington on Saturday and come back Sunday so he could be here in Seattle. And we also ask Mr. Willemssen to join us at each panel in the dialog, because he can pull it together on a national experience and relate it for us in what he has heard in this particular series of experiences.

So Mr. Willemssen, Director of Civil Agencies Information Systems, General Accounting Office, we're delighted to have you start the panel.

STATEMENTS OF JOEL C. WILLEMSSEN, DIRECTOR, CIVIL AGENCIES INFORMATION SYSTEMS, GENERAL ACCOUNTING OFFICE; CHRIS HEDRICK, DIRECTOR, WASHINGTON STATE YEAR 2000 OFFICE; CLIF BURWELL, Y2K PROGRAM MANAGER, KING COUNTY, WA; MARTY CHAKOIAN, PROJECT MANAGER, CITY OF SEATTLE YEAR 2000 OFFICE; AND BARBARA GRAFF, EMERGENCY PREPAREDNESS MANAGER, CITY OF BELLEVUE, WA

Mr. WILLEMSSEN. Thank you.

Mr. Chairman, Congresswoman, Congressman, thank you for inviting GAO to testify today. As requested, I'll briefly summarize our statement on the readiness of the Federal Government, State and local governments, and key economic sectors.

Regarding the Federal Government, reports indicate continued progress in fixing, testing, and implementing mission-critical systems. Nevertheless, numerous critical systems must still be made compliant, and must undergo independent verification and validation. The most recent agency quarterly reports, which were due to OMB last Friday, should provide us more updated information on where the Federal Government stands.

Our own reviews of selected agencies have shown uneven progress and remaining risks in addressing Y2K, and therefore point to the importance of business continuity and contingency planning. Even for those agencies that have clearly been Federal leaders, such as the Social Security Administration, some work remains to ensure full readiness.

If we look beyond individual agencies and individual systems, the Federal Government's future actions in the months remaining will need to be increasingly focused on making sure that its highest priority programs are year 2000 compliant. In line with this, OMB has identified 43 high-impact priorities, such as Medicare and food safety.

Available information on the Y2K readiness of State and local governments indicates that much work remains. For example, according to recently reported information on States, about eight States had completed implementing less than 75 percent of their mission-critical systems. Further, while all States responding said that they were engaged in contingency planning, 14 reported their deadlines for this as October or later.

Another area of risk is represented by Federal human services programs administered by States, programs such as Medicaid, food stamps, child support enforcement, unemployment insurance.

OMB-reported data on the systems supporting those programs show that numerous States are not planning to be ready until later this calendar year. Further, this is based on data that has not been independently verified.

Recent reports have also highlighted Y2K concerns at the local government level. For example, last month we reported on the Y2K status of the 21 largest U.S. cities. On average, these cities reported completing work for 45 percent of their key services.

Y2K is also a challenge for the public infrastructure and key economic sectors. Among the areas most at risk are health care and education.

For health care, we've testified on numerous occasions on the risks facing Medicare, Medicaid, and biomedical equipment. In addition, last month we reported that while many surveys had been completed on the Y2K readiness of health care providers, none of the eleven surveys we reviewed provided sufficient information to assess the true status of providers nationwide.

For education, this month's report of the President's Council on Y2K Conversion indicates that this continues to be an area of concern. For example, according to the Council report, many school districts could have dysfunctional information systems because less than one-third of institutions were reporting that their systems were compliant.

Mr. Chairman, that completes the summary of my statement. Thank you again for the opportunity. And after the panel is done, I'll be pleased to answer any questions.

[The prepared statement of Mr. Willemssen follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
9:00 a.m. PDT
Tuesday,
August 17, 1999

YEAR 2000 COMPUTING CHALLENGE

Readiness Improving Yet Essential Actions Remain to Ensure Delivery of Critical Services

Statement of Joel C. Willemssen
Director, Civil Agencies Information Systems
Accounting and Information Management Division

GAO
Accountability * Integrity * Reliability

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting us to participate in today's hearing on the Year 2000 problem. According to the report of the President's Commission on Critical Infrastructure Protection, the United States--with close to half of all computer capacity and 60 percent of Internet assets--is the world's most advanced and most dependent user of information technology.[1] Should these systems--which perform functions and services critical to our nation--suffer problems, it could create widespread disruption. Accordingly, the upcoming change of century is a sweeping and urgent challenge for public- and private-sector organizations alike.

Because of its urgent nature and the potentially devastating impact it could have on critical government operations, in February 1997 we designated the Year 2000 problem a high-risk area for the federal government.[2] Since that time, we have issued over 130 reports and testimony statements detailing specific findings and numerous recommendations related to the Year 2000 readiness of a wide range of federal agencies.[3] We have also issued guidance to help organizations successfully address the issue.[4]

Today I will highlight the Year 2000 risks facing the nation; discuss the federal government's progress and challenges that remain in correcting its systems; identify state and local government Year 2000 issues; and provide an overview of available information on the readiness of key public infrastructure and economic sectors.

[1] Critical Foundations: Protecting America's Infrastructures (President's Commission on Critical Infrastructure Protection, October 1997).

[2] High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

[3] A list of these publications is included as an attachment to this statement. These publications can be obtained through GAO's World Wide Web page at *www.gao.gov/y2kr.htm.*

[4] Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, issued as an exposure draft in February 1997 and in final form in September 1997), which addresses the key tasks needed to complete each phase of a Year 2000 program (awareness, assessment, renovation, validation, and implementation); Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, issued as an exposure draft in March 1998 and in final form in August 1998), which describes the tasks needed to ensure the continuity of agency operations; and Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, issued as an exposure draft in June 1998 and in final form in November 1998), which discusses the need to plan and conduct Year 2000 tests in a structured and disciplined fashion.

THE PUBLIC FACES RISK OF YEAR 2000 DISRUPTIONS

The public faces the risk that critical services provided by the government and the private sector could be severely disrupted by the Year 2000 computing problem. Financial transactions could be delayed, flights grounded, power lost, and national defense affected. Moreover, America's infrastructures are a complex array of public and private enterprises with many interdependencies at all levels. These many interdependencies among governments and within key economic sectors could cause a single failure to have adverse repercussions in other sectors. Key sectors that could be seriously affected if their systems are not Year 2000 compliant include information and telecommunications; banking and finance; health, safety, and emergency services; transportation; power and water; and manufacturing and small business.

The following are examples of some of the major disruptions the public and private sectors could experience if the Year 2000 problem is not corrected.

- With respect to aviation, there could be grounded or delayed flights, degraded safety, customer inconvenience, and increased airline costs.[5]

- Aircraft and other military equipment could be grounded because the computer systems used to schedule maintenance and track supplies may not work. Further, the Department of Defense could incur shortages of vital items needed to sustain military operations and readiness.[6]

- Medical devices and scientific laboratory equipment may experience problems beginning January 1, 2000, if their software applications or embedded chips use two-digit fields to represent the year.

Recognizing the seriousness of the Year 2000 problem, on February 4, 1998, the President signed an executive order that established the President's Council on Year 2000 Conversion, chaired by an Assistant to the President and consisting of one representative from each of the executive departments and from other federal agencies as may be determined by the Chair. The Chair of the Council was tasked with the following Year 2000 roles: (1) overseeing the activities of agencies; (2) acting as chief spokesperson in national and international forums; (3) providing policy coordination of executive branch activities with state, local, and tribal governments; and (4) promoting appropriate federal roles with respect to private-sector activities.

[5] FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998) and Year 2000 Computing Crisis: FAA Is Making Progress But Important Challenges Remain (GAO/T-AIMD/RCED-99-118, March 15, 1999).

[6] Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998).

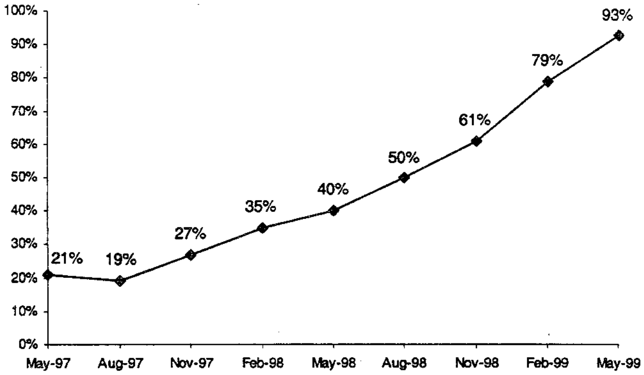
IMPROVEMENTS MADE BUT MUCH WORK REMAINS

Addressing the Year 2000 problem is a tremendous challenge for the federal government. Many of the federal government's computer systems were originally designed and developed 20 to 25 years ago, are poorly documented, and use a wide variety of computer languages, many of which are obsolete. Some applications include thousands, tens of thousands, or even millions of lines of code, each of which must be examined for date-format problems.

To meet this challenge and monitor individual agency efforts, the Office of Management and Budget (OMB) directed the major departments and agencies to submit quarterly reports on their progress, beginning May 15, 1997. These reports contain information on where agencies stand with respect to the assessment, renovation, validation, and implementation of mission-critical systems, as well as other management information on items such as costs and business continuity and contingency plans.

The federal government's most recent reports show improvement in addressing the Year 2000 problem. While much work remains, the federal government has significantly increased its percentage of mission-critical systems that are reported to be Year 2000 compliant, as chart 1 illustrates. In particular, while the federal government did not meet its goal of having all mission-critical systems compliant by March 1999, as of mid-May 1999, 93 percent of these systems were reported compliant.

Chart 1: Mission-Critical Systems Reported Year 2000 Compliant, May 1997-May 1999



Source: May 1997 – May 1999 data are from the OMB quarterly reports.

While this reported progress is notable, OMB also noted that 10 agencies have mission-critical systems that were not yet compliant.[7] In addition, as we testified in April, some of the systems that were not yet compliant support vital government functions.[8] For example, some of the systems that were not compliant were among the 26 mission-critical systems that the Federal Aviation Administration (FAA) has identified as posing the greatest risk to the National Airspace System—the network of equipment, facilities, and information that supports U.S. aviation operations.

Additionally, not all systems have undergone an independent verification and validation process. For example, in April 1999 the Department of Commerce awarded a contract for independent verification and validation reviews of approximately 40 mission-critical systems that support that Department's most critical business processes. These reviews are to continue through the summer of 1999. In some cases, independent verification and validation of compliant systems have found serious problems. For example, as we testified this past February,[9] none of 54 external mission-critical systems of the Health Care Financing Administration reported by the Department of Health and Human Services (HHS) as compliant as of December 31, 1998, was Year 2000 ready at that time, based on serious qualifications identified by the independent verification and validation contractor.

Reviews Show Uneven Federal Agency Progress

While the overall Year 2000 readiness of the government has improved, our reviews of federal agency Year 2000 programs have found uneven progress. Some agencies had made good progress while other agencies were significantly behind schedule but had taken actions to improve their readiness. For example:

- In October 1997, we reported that while SSA had made significant progress in assessing and renovating mission-critical mainframe software, certain areas of risk in its Year 2000 program remained.[10] Accordingly, we made several recommendations to address these risk areas, which included the Year 2000 compliance of the systems used by the 54 state Disability Determination Services[11] that help administer the disability programs. SSA agreed with these recommendations and, in July 1999, we

[7] The 10 agencies were the Departments of Agriculture, Commerce, Defense, Energy, Health and Human Services, Justice, Transportation, Treasury; the National Aeronautics and Space Administration; and the U.S. Agency for International Development.

[8] Year 2000 Computing Challenge: Federal Government Making Progress But Critical Issues Must Still Be Addressed to Minimize Disruptions (GAO/T-AIMD-99-144, April 14, 1999).

[9] Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services (GAO/T-AIMD-99-92, February 26, 1999).

[10] Social Security Administration: Significant Progress Made in Year 2000 Effort, But Key Risks Remain (GAO/AIMD-98-6, October 22, 1997).

[11] These include the systems in all 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.

reported that actions to implement these recommendations had either been taken or were underway.[12] For example, regarding the state Disability Determination Services systems, SSA enhanced its monitoring and oversight by establishing a full-time project team, designating project managers and coordinators, and requesting bi-weekly reports. While actions such as these demonstrated SSA's leadership in addressing the Year 2000 problem, it still needed to complete critical tasks to ensure readiness, including (1) ensuring the compliance of all external data exchanges, (2) completing tasks outlined in its contingency plans, (3) certifying the compliance of one remaining mission-critical system, (4) completing hardware and software upgrades in the Office of Telecommunications and Systems Operations, and (5) correcting date field errors identified through its quality assurance process.

- In May 1999 we testified[13] that the Department of Education had made progress toward addressing the significant risks we had identified in September 1998[14] related to systems testing, exchanging data with internal and external partners, and developing business continuity and contingency plans. Nevertheless, work remained ongoing in these areas. For example, Education had scheduled a series of tests with its data exchange partners, such as schools, through the early part of the fall. Tests such as these are important since Education's student financial aid environment is very large and complex, including over 7,000 schools, 6,500 lenders, and 36 guaranty agencies, as well as other federal agencies; we have reported that Education has experienced serious data integrity problems in the past.[15] Accordingly, our May testimony stated that Education needed to continue end-to-end testing of critical business processes involving Education's internal systems and its external data exchange partners and continue its outreach activities with schools, guaranty agencies, and other participants in the student financial aid community.

- Our work has shown that the Department of Defense and the military services face significant problems.[16] This March we testified that, despite considerable progress made in the preceding 3 months, the department was still well behind schedule.[17] We found that the Department of Defense faced two significant challenges: (1)

[12] Social Security Administration: Update on Year 2000 and Other Key Information Technology Initiatives (GAO/T-AIMD-99-259, July 29, 1999).
[13] Year 2000 Computing Challenge: Education Taking Needed Actions But Work Remains (GAO/T-AIMD-99-180, May 12, 1999).
[14] Year 2000 Computing Crisis: Significant Risks Remain to Department of Education's Student Financial Aid Systems (GAO/T-AIMD-98-302, September 17, 1998).
[15] Student Financial Aid Information: Systems Architecture Needed to Improve Programs' Efficiency (GAO/AIMD-97-122, July 29, 1997).
[16] Defense Computers: Year 2000 Computer Problems Put Navy Operations At Risk (GAO/AIMD-98-150, June 30, 1998); Defense Computers: Army Needs to Greatly Strengthen Its Year 2000 Program (GAO/AIMD-98-53, May 29, 1998); GAO/AIMD-98-72, April 30, 1998; and Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998).
[17] Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed (GAO/T-AIMD-99-101, March 2, 1999).

completing remediation and testing of its mission-critical systems and (2) having a reasonable level of assurance that key processes will continue to work on a day-to-day basis and key operational missions necessary for national defense can be successfully accomplished. We concluded that such assurance could only be provided if Defense took steps to improve its visibility over the status of key business processes.

End-To-End Testing Must Be Completed

While it is important to achieve compliance for individual mission-critical systems, realizing such compliance alone does not ensure that business functions will continue to operate through the change of century—the ultimate goal of Year 2000 efforts. The purpose of end-to-end testing is to verify that a defined set of interrelated systems, which collectively support an organizational core business area or function, will work as intended in an operational environment. In the case of the year 2000, many systems in the end-to-end chain will have been modified or replaced. As a result, the scope and complexity of testing--and its importance--are dramatically increased, as is the difficulty of isolating, identifying, and correcting problems. Consequently, agencies must work early and continually with their data exchange partners to plan and execute effective end-to-end tests. (Our Year 2000 testing guide sets forth a structured approach to testing, including end-to-end testing.)[18]

In January we testified that with the time available for end-to-end testing diminishing, OMB should consider, for the government's most critical functions, setting target dates, and having agencies report against them, for the development of end-to-end test plans, the establishment of test schedules, and the completion of the tests.[19] On March 31, OMB and the Chair of the President's Council on Year 2000 Conversion announced that one of the key priorities that federal agencies will be pursuing during the rest of 1999 will be cooperative end-to-end testing to demonstrate the Year 2000 readiness of federal programs with states and other partners.

Agencies have also acted to address end-to-end testing. For example, our March FAA testimony[20] found that the agency had addressed our prior concerns about the lack of detail in its draft end-to-end test program plan and had developed a detailed end-to-end testing strategy and plans.[21] Also, in June 1999 we reported[22] that the Department of Defense had underway or planned hundreds of related Year 2000 end-to-end test and evaluation activities and that, thus far, it was taking steps to ensure that these related end-to-end tests were effectively coordinated. However, we concluded that the Department of

[18] GAO/AIMD-10.1.21, November 1998.

[19] Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, January 20, 1999).

[20] GAO/T-AIMD/RCED-99-118, March 15, 1999.

[21] GAO/T-AIMD-98-251, August 6, 1998.

[22] Defense Computers: Management Controls Are Critical To Effective Year 2000 Testing (GAO/AIMD-99-172, June 30, 1999).

Defense was far from successfully finishing its various Year 2000 end-to-end test activities and that it must complete efforts to establish end-to-end management controls, such as establishing an independent quality assurance program.

Business Continuity and Contingency Plans Are Needed

Business continuity and contingency plans are essential. Without such plans, when unpredicted failures occur, agencies will not have well-defined responses and may not have enough time to develop and test alternatives. Federal agencies depend on data provided by their business partners as well as on services provided by the public infrastructure (e.g., power, water, transportation, and voice and data telecommunications). One weak link anywhere in the chain of critical dependencies can cause major disruptions to business operations. Given these interdependencies, it is imperative that contingency plans be developed for all critical core business processes and supporting systems, regardless of whether these systems are owned by the agency. Accordingly, in April 1998 we recommended that the Council require agencies to develop contingency plans for all critical core business processes.[23]

OMB has clarified its contingency plan instructions and, along with the Chief Information Officers Council, has adopted our business continuity and contingency planning guide.[24] In particular, on January 26, 1999, OMB called on federal agencies to identify and report on the high-level core business functions that are to be addressed in their business continuity and contingency plans, as well as to provide key milestones for development and testing of such plans in their February 1999 quarterly reports. In addition, on May 13 OMB required agencies to submit high-level versions of these plans by June 15. According to an OMB official, OMB has received plans from the 24 major departments and agencies. This official stated that OMB planned to review the plans, discuss them with the agencies, determine whether there were any common themes, and report on the plans' status in its next quarterly report.

To provide assurance that agencies' business continuity and contingency plans will work if needed, on January 20 we suggested that OMB may want to consider requiring agencies to test their business continuity strategy and set a target date, such as September 30, 1999, for the completion of this validation.[25] Our review of the 24 major departments and agencies' May 1999 quarterly reports found 14 cases in which agencies did not identify test dates for their business continuity and contingency plans or reported test dates subsequent to September 30, 1999.

On March 31, OMB and the Chair of the President's Council announced that completing and testing business continuity and contingency plans as insurance against disruptions to federal service delivery and operations from Year 2000-related failures will be one of the

[23] Year 2000 Computing Crisis: Potential for Widespread Disruption Calls for Strong Leadership and Parternships (GAO/AIMD-98-85, April 30, 1998).

[24] GAO/AIMD-10.1.19, August 1998.

[25] GAO/T-AIMD-99-50, January 20, 1999.

key priorities that federal agencies will be pursuing through the rest of 1999. Accordingly, OMB should implement our suggestion and establish a target date for the validation of agency business continuity and contingency plans.

Our reviews of specific agency business continuity and contingency plans have found that agencies are in varying stages of completion. For example,

- We testified in July 1999 that SSA was in the process of testing all of its contingency plans, with expected completion in September.[26] In addition, SSA planned to assist the Department of the Treasury in developing alternative disbursement processes for problematic financial institutions.

- This June, we testified that the U. S. Customs Service had implemented sound management processes for developing business continuity and contingency plans and was in the process of testing its plans.[27] Customs expected to complete contingency plan testing by October 1999.

- In May 1999, we reported[28] that the Department of Agriculture's component agencies were actively engaged in developing business continuity and contingency plans but that much work remained to complete and test these plans. Further, its December 1999 departmentwide goal of completing business continuity and contingency plans left no room for delays or sufficient time for correcting, revising, and retesting plans, if necessary. Consequently, we recommended that the Department of Agriculture advance its time frame to no later than September 30, 1999, and develop priorities for completing and testing business continuity and contingency plans that are aligned with the department's highest priority business processes, to ensure that remaining work addresses these processes first. The Department of Agriculture's Chief Information Officer stated that the department planned to implement our recommendations.

- This June, we reported[29] that the General Services Administration had completed its telecommunications business continuity and contingency plan in September 1998. However, we made several suggestions for enhancing this plan, including that the General Services Administration work with its customers to ensure that the customers' business continuity and contingency plans are fully coordinated with the General Services Administration's plan and that it consider the possibility of partial loss of service. The General Services Administration agreed to implement our suggestions.

[26] GAO/T-AIMD-99-259, July 29, 1999.

[27] Year 2000 Computing Crisis: Customs Is Making Good Progress (GAO/T-AIMD-99-225, June 29, 1999).

[28] Year 2000 Computing Crisis: USDA Needs to Accelerate Time Frames for Completing Contingency Planning (GAO/AIMD-99-178, May 21, 1999).

[29] GSA's Effort to Develop Year 2000 Business Continuity and Contingency Plans for Telecommunications Systems (GAO/AIMD-99-201R, June 16, 1999).

OMB Action Could Help Ensure Business Continuity of High-Impact Programs

While individual agencies have been identifying and remediating mission-critical systems, the government's future actions need to be focused on its high-priority programs and ensuring the continuity of these programs, including the continuity of federal programs that are administered by states. Accordingly, governmentwide priorities need to be based on such criteria as the potential for adverse health and safety effects, adverse financial effects on American citizens, detrimental effects on national security, and adverse economic consequences. In April 1998 we recommended that the President's Council on Year 2000 Conversion establish governmentwide priorities and ensure that agencies set agencywide priorities.[30]

On March 26, OMB implemented our recommendation by issuing a memorandum to federal agencies designating lead agencies for the government's 42 high-impact programs (e.g., food stamps, Medicare, and federal electric power generation and delivery). (OMB later added a 43rd high-impact program—the Department of Justice's National Crime Information Center.) Appendix I lists these programs and their lead agencies. For each program, the lead agency was charged with identifying to OMB the partners integral to program delivery; taking a leadership role in convening those partners; assuring that each partner has an adequate Year 2000 plan and, if not, helping each partner without one; and developing a plan to ensure that the program will operate effectively. According to OMB, such a plan might include testing data exchanges across partners, developing complementary business continuity and contingency plans, sharing key information on readiness with other partners and the public, and taking other steps necessary to ensure that the program will work. OMB directed the lead agencies to provide a schedule and milestones of key activities in their plans by April 15. OMB also asked agencies to provide monthly progress reports. As you know, we are currently reviewing agencies' progress in ensuring the readiness of their high-impact programs for this subcommittee.

STATE AND LOCAL GOVERNMENTS FACE SIGNIFICANT YEAR 2000 RISKS

Just as the federal government faces significant Year 2000 risks, so too do state and local governments. If the Year 2000 problem is not properly addressed, for example, (1) food stamps and other types of payments may not be made or could be made for incorrect amounts; (2) date-dependent signal timing patterns could be incorrectly implemented at highway intersections, with safety severely compromised; and (3) prisoner release or parole eligibility determinations may be adversely affected. Nevertheless, available information on the Year 2000 readiness of state and local governments indicates that much work remains.

[30] GAO/AIMD-98-85, April 30, 1998.

According to information on state Year 2000 activities reported to the National Association of State Information Resource Executives as of August 3, 1999,[31] states[32] reported having thousands of mission-critical systems.[33] With respect to completing the implementation phase for these systems,

- 2 states[34] reported that they had completed between 25 and 49 percent,
- 6 states[35] reported completing between 50 and 74 percent,
- 38 states[36] reported completing between 75 and 99 percent, and
- 3 states reported completing the implementation phase for all mission-critical systems.[37]

All of the states responding to the National Association of State Information Resource Executives survey reported that they were actively engaged in internal and external contingency planning and that they had established target dates for the completion of these plans; 14 (28 percent) reported the deadline as October 1999 or later.

State audit organizations have also identified significant Year 2000 concerns. In January, the National State Auditors Association reported on the results of its mid-1998 survey of Year 2000 compliance among states.[38] This report stated that, for the 12 state audit organizations that provided Year 2000-related reports, concerns had been raised in areas such as planning, testing, embedded systems, business continuity and contingency planning, and the adequacy of resources to address the problem.

We identified additional products by 17 state-level audit organizations and Guam that

[31] Individual states submit periodic updates to the National Association of State Information Resource Executives. For the August 3 report, over three quarters of the states submitted their data after July 1, 1999. The oldest data were provided on March 11 and the most recent data on August 2.
[32] In the context of the National Association of State Information Resource Executives survey, the term "states" includes the District of Columbia and Puerto Rico.
[33] Mission-critical systems were defined as those that a state had identified as priorities for prompt remediation.
[34] One state reported on its mission-critical systems and one state reported on its processes.
[35] Five states reported on their mission-critical systems and one reported on all systems.
[36] Thirty-one states reported on their mission-critical systems, two states reported on their applications, one reported on its "priority business activities," one reported on its "critical compliance units," one reported on all systems, one reported on functions, and one reported on projects.
[37] Two states did not respond to the survey and one did not respond to this question.
[38] Year 2000: State Compliance Efforts (National State Auditors Association, January 1999).

discussed the Year 2000 problem and that had been issued since October 1, 1998. Several of these state-level audit organizations noted that progress had been made. However, the audit organizations also expressed concerns that were consistent with those reported by the National State Auditors Association. For example:

- In December 1998 the Vermont State Auditor reported[39] that the state Chief Information Officer did not have a comprehensive control list of the state's information technology systems. Accordingly, the audit office stated that, even if all mission-critical state systems were checked, these systems could be endangered by information technology components that had not been checked or by linkages with the state's external electronic partners.

- In April, New York's Division of Management Audit and State Financial Services reported that state agencies did not adequately control the critical process of testing remediated systems.[40] Further, most agencies were in the early stages of addressing potential problems related to data exchanges and embedded systems and none had completed substantive work on contingency planning. The New York audit office subsequently issued 27 reports on individual mission-critical and high-priority systems that included concerns about, for example, contingency planning and testing.

- In February, the California State Auditor reported[41] that key agencies responsible for emergency services, corrections, and water resources, among other areas, had not fully addressed embedded technology-related threats. Regarding emergency services, the California report stated that if remediation of the embedded technology in its networks were not completed, the Office of Emergency Services might have to rely on cumbersome manual processes, significantly increasing response time to disasters.

- In March, Oregon's Audits Division reported[42] that 11 of the 12 state agencies reviewed did not have business continuity plans addressing potential Year 2000 problems for their core business functions.

[39] Vermont State Auditor's Report on State Government's Year 2000 Preparedness (Y2K Compliance) for the Period Ending November 1, 1998 (Office of the State Auditor, December 31, 1998).

[40] New York's Preparation for the Year 2000: A Second Look (Office of the State Comptroller, Division of Management Audit and State Financial Services, Report 98-S-21, April 5, 1999).

[41] Year 2000 Computer Problem: The State's Agencies Are Progressing Toward Compliance but Key Steps Remain Incomplete (California State Auditor, February 18, 1999).

[42] Department of Administrative Services Year 2000 Statewide Project Office Review (Secretary of State, Audits Division, State of Oregon Report No. 99-05, March 16, 1999).

- In March, North Carolina's State Auditor reported[43] that resource restrictions had limited the state's Year 2000 Project Office's ability to verify data reported by state agencies.

It is also essential that local government systems be ready for the change of century since critical functions involving, for example, public safety and traffic management, are performed at the local level. Recent reports on local governments have highlighted Year 2000 concerns. For example:

- On July 15, we reported on the reported Year 2000 status of the 21 largest U.S. cities.[44] On average, cities reported completing work for 45 percent of the key service areas in which they have responsibility. In addition, two cities reported that they had completed their Year 2000 efforts, nine cities expected to complete their Year 2000 preparations by September 30, 1999, and the remaining 10 cities expected to complete their preparation by December 31.[45] In addition, 7 cities reported completing Year 2000 contingency plans, while 14 cities reported that their plans were still being developed.

- On July 9, the National League of Cities reported on its survey of 403 cities conducted in April 1999. This survey found that (1) 92 percent of cities had a citywide Year 2000 plan, (2) 74 percent had completed their assessment of critical systems, and (3) 66 percent had prepared contingency plans. (Of those that had not completed such plans, about half stated that they were planning to develop one.) In addition, 92 percent of the cities reported that they expect that all of their critical systems will be compliant by January 1, 2000; 5 percent expected to have completed between 91 and 99 percent, and 3 percent expected to have completed between 81 and 90 percent of their critical systems by January 1.

- On June 23, the National Association of Counties announced the results of its April survey of 500 randomly selected counties. This survey found that (1) 74 percent of respondents had a countywide plan to address Year 2000 issues, (2) 51 percent had completed system assessments, and (3) 27 percent had completed system testing. In addition, 190 counties had prepared contingency plans and 289 had not. Further, of the 114 counties reporting that they planned to develop Year 2000 contingency plans, 22 planned to develop the plan in April-June, 64 in July-September, 18 in October-December, and 10 did not yet know.

[43] Department of Commerce, Information Technology Services Year 2000 Project Office (Office of the State Auditor, State of North Carolina, March 18, 1999).
[44] Reported Y2K Status of the 21 Largest U.S. Cities (GAO/AIMD-99-246R, July 15, 1999).
[45] In most cities, the majority of city services are scheduled to be completed before this completion date. For example, Los Angeles plans to have all key city systems ready by September 30, except for its wastewater treatment systems, which are expected to be completed in November.

Of critical importance to the nation are services essential to the safety and well-being of individuals across the country, namely 9-1-1 systems and law enforcement. For the most part, responsibility for ensuring continuity of service for 9-1-1 calls and law enforcement resides with thousands of state and local jurisdictions. On April 29 we testified that not enough was known about the status of either 9-1-1 systems or of state and local law enforcement activities to conclude about either's ability during the transition to the year 2000 to meet the public safety and well-being needs of local communities across the nation.[46] While the federal government planned additional actions to determine the status of these areas, we stated that the President's Council on Year 2000 Conversion should use such information to identify specific risks and develop appropriate strategies and contingency plans to respond to those risks.

We subsequently reported[47] that the Federal Emergency Management Agency and the Department of Justice have worked to increase the response rate to a survey of public safety organizations. As of June 30, 1999, of the over 2,200 9-1-1 sites responding (about half of the 9-1-1 call answering sites in the United States), 37 percent reported that they were ready for the Year 2000. Another 55 percent responded that they expected to be Year 2000 compliant in time for the change of century.

Recognizing the seriousness of the Year 2000 risks facing state and local governments, the President's Council has developed initiatives to address the readiness of state and local governments. For example:

- The Council established working groups on state and local governments and tribal governments.
- Council officials participate in monthly multistate conference calls.
- In July 1998 and March 1999, the Council, in partnership with the National Governors' Association, convened Year 2000 summits with state and U.S. territory Year 2000 coordinators.
- On May 24, the Council announced a nationwide campaign to promote "Y2K Community Conversations" to support and encourage efforts of government officials, business leaders, and interested citizens to share information on their progress. To support this initiative, the Council has developed and is distributing a toolkit that provides examples of which sectors should be represented at these events and issues that should be addressed.

[46] Year 2000 Computing Challenge: Status of Emergency and State and Local Law Enforcement Systems Is Still Unknown (GAO/T-AIMD-99-163, April 29, 1999).
[47] Emergency and State and Local Law Enforcement Systems: Committee Questions Concerning Year 2000 Challenges (GAO/AIMD-99-247R, July 14, 1999).

State-Administered Federal Human Services Programs Are At Risk

Among the critical functions performed by states are the administration of federal human services programs. As we reported in November 1998, many systems that support state-administered federal human services programs were at risk, and much work remained to ensure that services would continue.[48] In February of this year, we testified that while some progress had been achieved, many states' systems were not scheduled to become compliant until the last half of 1999.[49] Accordingly, we concluded that, given these risks, business continuity and contingency planning was even more important in ensuring continuity of program operations and benefits in the event of systems failures.

Subsequent to our November 1998 report, OMB directed federal oversight agencies to include the status of selected state human services systems in their quarterly reports. Specifically, in January 1999, OMB requested that agencies describe actions to help ensure that federally supported, state-run programs will be able to provide services and benefits. OMB further asked that agencies report the date when each state's systems will be Year 2000-compliant.

Table 1 summarizes the latest information on state-administered federal human services programs reported by OMB on June 15, 1999.[50] This information was gathered, but not verified, by the Departments of Agriculture, HHS, and Labor.[51] It indicates that while many states reported their programs to be compliant, a number of states did not plan to complete Year 2000 efforts until the last quarter of 1999. For example, eight states did not expect to be compliant until the last quarter of 1999 for Child Support Enforcement, five states for Unemployment Insurance, and four states for Child Nutrition. Moreover, Year 2000 readiness information was unknown in many cases. For example, according to OMB, the status of 32 states' Low Income Home Energy Assistance programs was unknown because applicable readiness information was not available.

[48] Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998).

[49] Year 2000 Computing Crisis: Readiness of State Automated Systems That Support Federal Human Services Programs (GAO/T-AIMD-99-91, February 24, 1999).

[50] For Medicaid, OMB reports on the two primary systems that states use to administer the program: (1) the Integrated Eligibility System, to determine whether an individual applying for Medicaid meets the eligibility criteria for participation, and (2) the Medicaid Management Information System, to process claims and deliver payments for services rendered. Integrated eligibility systems are also often used to determine eligibility for other public assistance programs, such as Food Stamps.

[51] The Department of Agriculture oversees the Child Nutrition, Food Stamp, and the Women, Infants, and Children programs. HHS oversees the Child Care, Child Support Enforcement, Child Welfare, Low Income Home Energy Assistance, Medicaid, and Temporary Assistance for Needy Families programs. The Department of Labor oversees the Unemployment Insurance program.

Table 1: Reported State-level Readiness for Federally Supported Programs[a]

		Expected Date of 1999 Compliance					
Program[b]	Compliant[c]	Jan.-March	April-June	July-Sept.	Oct.-Dec.	Unk.[d]	N/A[e]
Child Nutrition	29	0	9	10	4	2	0
Food Stamps	25	0	12	14	3	0	0
Women, Infants, and Children	33	0	11	7	3	0	0
Child Care	24	5	5	8	2	6	4
Child Support Enforcement	15	4	13	8	8	6	0
Child Welfare	20	5	9	11	3	5	1
Low Income Home Energy Assistance Program	10	0	3	7	1	32	1
Medicaid – Integrated Eligibility System	20	0	15	15	4	0	0
Medicaid – Management Information System	17	0	19	14	4	0	0
Temporary Assistance for Needy Families	19	3	12	15	1	4	0
Unemployment Insurance	27	0	11	10	5	0	1

[a] This chart contains readiness information from the 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands.

[b] According to OMB, the information regarding Child Care, Child Support Enforcement, the Low Income Home Energy Assistance Program, Medicaid, and Temporary Assistance for Needy Families was as of January 31, 1999; and the information for Child Nutrition, Food Stamps, and Women, Infants and Children was as of March 1999. However, OMB provided a draft table to the National Association of State Information Resource Executives which, in turn, provided the draft table to the states. The states were asked to contact HHS and Agriculture and provide corrections by June 1, 1999. For their part, HHS and Agriculture submitted updated state data to OMB in early June. The information regarding Unemployment Insurance was as of March 31, 1999.

[c] In many cases, the report indicated a date instead of whether the state was compliant. We assumed that states reporting completion dates in 1998 or earlier were compliant.

[d] Unknown indicates that, according to OMB, the data reported by the states were unclear or that no information was reported by the agency.

[e] N/A indicates that the states or territories reported that the data requested were not applicable to them.

Source: Progress on Year 2000 Conversion: 9th Quarterly Report (OMB, issued on June 15, 1999).

Although many states have reported their state-administered programs to be compliant, additional work beyond individual system completion likely remains, such as end-to-end testing. For example, of the states that OMB reported as having compliant Medicaid management information and/or integrated eligibility systems, at least four and five states, respectively, had not completed end-to-end testing.

In addition to obtaining state-reported readiness status information for OMB, the three federal departments are taking other actions to assess the ability of state-administered programs to continue into the next century. However, as table 2 shows, the approaches of the three departments in assessing the readiness of state-administered federal human services programs vary significantly. For example, HHS' Health Care Financing Administration (HCFA) hired a contractor to perform comprehensive on-site reviews in all states, some more than once, using a standard methodology. Agriculture's Food and Nutrition Service (FNS) approach includes such actions as having regional offices monitor state Year 2000 efforts and obtaining state certifications of compliance. The Department of Labor is relying on its regional offices to monitor state Year 2000 efforts as well as requiring states to obtain and submit an independent verification and validation report after declaring their systems compliant.

Table 2: Number and Types Of Assessments Performed

		Areas Covered By Assessments		
Agency/ Program	Number of States Assessed	Project Management/ Planning	Test Plans/ Results	Business Continuity and Contingency Plans (BCCP)
Agriculture/ Child Nutrition Program	Component entity's regional offices are monitoring all states' efforts	Varies by region	Varies by region	Varies by region
Agriculture/ Food Stamps	Component entity's regional offices are monitoring all states' efforts	Varies by region	Varies by region	Varies by region
Agriculture/ Women, Infants, and Children	Component entity's regional offices are monitoring all states' efforts	Varies by region	Varies by region	Varies by region
HHS/Child Care	As of July 2, a contractor had conducted on-site reviews of 20 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—on-site visits included reviews of states' BCCP processes, but not their content
HHS/Child Support Enforcement	As of July 2, a contractor had conducted on-site reviews of 20 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—on-site visits included reviews of states' BCCP processes, but not their content
HHS/Child Welfare	As of July 2, a contractor had conducted on-site reviews of 20 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—on-site visits included reviews of states' BCCP processes, but not their content
HHS/Low Income Housing Energy Assistance Program	As of July 2, a contractor had conducted on-site reviews of 20 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—on-site visits included reviews of states' BCCP processes, but not their content
HHS/Medicaid	A contractor conducted on-site reviews of 50 states and the District of Columbia once, and as of June 30, the contractor had conducted follow-up reviews of 14 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—Initial visits included a review of a state's BCCP process, and as of July 9, a contractor had reviewed the content of 42 states' BCCPs, either on site or at headquarters
HHS/ Temporary Assistance for Needy Families	As of July 2, a contractor had conducted on-site reviews of 20 states	Yes	Yes—all visits included reviews of test plans and, where applicable, test results	Partial—on-site visits included reviews of states' BCCP processes, but not their content
Labor/ Unemployment Insurance	Labor's regional offices are monitoring all states' efforts	Unknown—not specifically addressed in methodology	Unknown—not specifically addressed in methodology	Reviews ongoing

In addition to the completed reviews, all of the departments have ongoing initiatives to ensure that state-administered human services programs will continue to function past the change of century. These initiatives are part of the departments' overall strategies to ensure the continued delivery of these high-impact programs. For example,

- In June 1999, the Department of Agriculture's FNS required its regions to provide for each program a copy of either a state letter certifying that it was Year 2000 compliant or a business continuity and contingency plan. As of June 18, 1999, FNS had received (1) 9 certifications and 7 business continuity and contingency plans for Child Nutrition; (2) 12 certifications and 16 business continuity and contingency plans for Food Stamps; and (3) 23 certifications and 23 business continuity and contingency plans for Women, Infants, and Children. In addition, to help states' Year 2000 efforts, FNS employed a contractor to conduct on-site visits to 20 states for one or more programs. As of July 9, FNS officials told us 16 states had been visited. With respect to the scope of these visits, FNS' regional offices determine for each state and program what specific areas it should encompass. These visits are principally intended to provide technical assistance to the states in areas such as Year 2000 project management, hardware and software testing, and contingency planning.

- In its initial round of on-site reviews conducted between November 1998 and April 1999, the contractor hired by HHS' HCFA (1) identified barriers to successful remediation; (2) made recommendations to address specific areas of concern; and (3) placed Medicaid integrated eligibility and management information systems into low, medium, or high risk categories. HCFA's contractor is currently conducting a second round of on-site reviews in at least 40 states—primarily those in which at least one of two systems was categorized as a high or medium risk during the initial visit. As of June 30, 14 states had been visited during this round. The focus of this second round of visits is on determining how states have resolved Year 2000 issues previously identified, as well as reviewing activities such as data exchanges and end-to-end testing. HCFA plans to conduct a third round of on-site reviews in the fall of 1999 for those states that continue to have systems categorized as high risk. Additionally, another HCFA contractor is reviewing the content of all states' business continuity and contingency plans, with some of these reviews being performed in conjunction with the second round of state visits.

- In September 1998, the Department of Labor required that all State Employment Security Agencies conduct independent verification and validation reviews of their Unemployment Insurance programs. The department set a target date of July 1, 1999, for states to submit independent verification and validation certifications of their Unemployment Insurance systems to Labor's regional offices. Labor required its regional offices to review independent verification and validation reports and certifications of Year 2000 compliance that State Employment Security Agencies submitted, and ascertain whether the material met the department's requirements. If Labor's requirements were met, the regional offices were to approve the State Employment Security Agencies' certification and independent verification and validation reports and forward copies of the approved certification and report, along

with regional office comments, to Labor's national office.

An example of the benefits that federal/state partnerships can provide is illustrated by the Department of Labor's unemployment services program. In September 1998, we reported that many State Employment Security Agencies were at risk of failure as early as January 1999 and urged the Department of Labor to initiate the development of realistic contingency plans to ensure continuity of core business processes in the event of Year 2000-induced failures.[52] In May, we testified that four state agencies' systems could have failed if systems in those states had not been programmed with an emergency patch in December 1998. This patch was developed by several of the state agencies and promoted to other state agencies by the Department of Labor.[53]

YEAR 2000 READINESS INFORMATION AVAILABLE IN SOME SECTORS, BUT KEY INFORMATION STILL MISSING OR INCOMPLETE

Beyond the risks faced by federal, state, and local governments, the year 2000 also poses a serious challenge to the public infrastructure, key economic sectors, and to other countries. To address these concerns, in April 1998 we recommended that the Council use a sector-based approach and establish the effective public-private partnerships necessary to address this issue.[54] The Council subsequently established over 25 sector-based working groups and has been initiating outreach activities since it became operational last spring. In addition, the Chair of the Council has formed a Senior Advisors Group composed of representatives from private-sector firms across key economic sectors. Members of this group are expected to offer perspectives on cross-cutting issues, information sharing, and appropriate federal responses to potential Year 2000 failures.

Our April 1998 report also recommended that the President's Council develop a comprehensive picture of the nation's Year 2000 readiness, to include identifying and assessing risks to the nation's key economic sectors--including risks posed by international links. In October 1998 the Chair directed the Council's sector working groups to begin assessing their sectors. The Chair also provided a recommended guide of core questions that the Council asked to be included in surveys by the associations performing the assessments. These questions included the percentage of work that has been completed in the assessment, renovation, validation, and implementation phases. The Chair then planned to issue quarterly public reports summarizing these assessments.

[52] Year 2000 Computing Crisis: Progress Made at Department of Labor, But Key Systems at Risk (GAO/T-AIMD-98-303, September 17, 1998).
[53] Year 2000 Computing Challenge: Labor Has Progressed But Selected Systems Remain at Risk (GAO/T-AIMD-99-179, May 12, 1999).
[54] GAO/AIMD-98-85, April 30, 1998.

The Council's most recent report was issued on August 5, 1999.[55] The report stated that important national systems will make a successful transition to the year 2000 but that much work, such as contingency planning, remains to be done. In particular, the Council expressed a high degree of confidence in five major domestic areas: financial institutions, electric power, telecommunications, air travel, and the federal government. For example, the Council stated that on August 2, federal bank, thrift, and credit union regulators reported that 99 percent of federally insured financial institutions have completed testing of critical systems for Year 2000 readiness. The Council had concerns in four significant areas: local government, health care, education, and small businesses. For example, according to the Council report, many school districts could move into the new century with dysfunctional information technology systems, since only 28 percent and 30 percent of Superintendent/Local Educational Agencies and post-secondary institutions, respectively, reported that their mission-critical systems were Year 2000 compliant. Internationally, the Council stated that the Year 2000 readiness of other countries was improving but was still a concern. The Council reported that the June 1999 meeting of National Year 2000 Coordinators held at the United Nations found that the 173 countries in attendance were clearly focused on the Year 2000 problem but that many countries will likely not have enough time or resources to finish before the end of 1999.

The Council's assessment reports have substantially increased the nation's understanding of the Year 2000 readiness of key industries. However, the picture remains incomplete in certain key areas because the surveys conducted to date did not have a high response rate or did not provide their response rate; the assessment was general or contained projections rather than current remediation information; or the data were old. For example, according to the Council's latest assessment report,

- Less than a quarter of the more than 16,000 Superintendents of Schools/Local Educational Agencies responded to a web-based survey of Year 2000 readiness among elementary and secondary schools. Similarly, less than a third of the more than 6,000 presidents and/or chancellors of post-secondary educational institutions responded to a web-based Year 2000 survey. Also, surveys covering areas such as small and medium-sized chemical enterprises did not provide information on either the number of surveys distributed or the number returned. Small response rates or the lack of information on response rates call into question whether the results of the survey accurately portray the readiness of the sector.

- Information in areas, such as state emergency management and broadcast television and radio provided a general assessment or projected compliance levels as of a certain date, but did not contain detailed data as to the current status of the sector (e.g., the average percentage of organizations' systems that are Year 2000 compliant or the

[55] The Council's three reports are available on its web site, *www.y2k.gov*. In addition, the Council, in conjunction with the Federal Trade Commission and the General Services Administration, has established a toll-free Year 2000 information line, 1-888-USA-4Y2K. The Federal Trade Commission has also included Year 2000 information of interest to consumers on its web site, *www.consumer.gov*.

percentage of organizations that are in the assessment, renovation, or validation phases).

- In some cases, such as for grocery manufacturers, cable television, hospitals, physicians' practices, and railroads, the sector surveys had been conducted months earlier and/or current survey information was not yet available.

In addition to our work related to the federal, state, and local government's Year 2000 progress, we have also issued several products related to key economic sectors. I will now discuss the results of these reviews.

Energy Sector

In April, we reported that while the electric power industry had concluded that it had made substantial progress in making its systems and equipment ready to continue operations into the year 2000, significant risks remained since many reporting organizations did not expect to be Year 2000 ready within the June 1999 industry target date.[56] We, therefore, suggested that the Department of Energy (1) work with the Electric Power Working Group to ensure that remediation activities were accelerated for the utilities that expected to miss the June 1999 deadline for achieving Year 2000 readiness and (2) encourage state regulatory utility commissions to require a full public disclosure of Year 2000 readiness status of entities transmitting and distributing electric power. The Department of Energy generally agreed with our suggestions. We also suggested that the Nuclear Regulatory Commission (1) in cooperation with the Nuclear Energy Institute, work with nuclear power plant licensees to accelerate the Year 2000 remediation efforts among the nuclear power plants that expect to meet the June 1999 deadline for achieving readiness and (2) publicly disclose the Year 2000 readiness of each of the nation's operational nuclear reactors. In response, the Nuclear Regulatory Commission stated that it plans to focus its efforts on nuclear power plants that may miss the July 1, 1999 milestone and that it would release the readiness information on individual plants that same month.

Subsequent to our report, on August 3, 1999, the North American Electric Reliability Council released its fourth status report on electric power systems. According to the Council, as of June 30, 1999—the industry target date for organizations to be Year 2000 ready—251 of 268 (94 percent) of bulk electric organizations were Year 2000 ready or Year 2000 ready with limited exceptions.[57] In addition, this report stated that 96 percent

[56] Year 2000 Computing Crisis: Readiness of the Electric Power Industry (GAO/AIMD-99-114, April 6, 1999).

[57] The North American Electric Reliability Council reported that 64 of these organizations had exceptions but that it "believes that the work schedule provided to complete these exception items in the next few months represents a prudent use of resources and does not increase risks associated with reliable electric service into the Year 2000."

of local distribution systems were reported as Year 2000 ready.[58] The North American Electric Reliability Council stated that the information it uses is principally self-reported but that 84 percent of the organizations reported that their Year 2000 programs had also been audited by internal and/or external auditors. On July 19, the Nuclear Regulatory Commission stated that 68 of 103 (66 percent) nuclear power plants reported that all of their computer systems and digital embedded components that support plant operations are Year 2000 ready. Of the 35 plants that were not Year 2000 ready, 18 had systems or components that were not ready that could affect power generation.

In May, we reported[59] that while the domestic oil and gas industries had reported that they had made substantial progress in making their equipment and systems ready to continue operations into the year 2000, risks remained. For example, although over half of our oil is imported, little was known about the Year 2000 readiness of foreign oil suppliers. Further, while individual domestic companies reported that they were developing Year 2000 contingency plans, there were no plans to perform a national-level risk assessment and develop contingency plans to deal with potential shortages or disruptions in the nation's overall oil and gas supplies. We suggested that the Council's oil and gas working group (1) work with industry associations to perform national-level risk assessments and develop and publish credible, national-level scenarios regarding the impact of potential Year 2000 failures and (2) develop national-level contingency plans. The working group generally agreed with these suggestions.

Water Sector

In April we reported[60] that insufficient information was available to assess and manage Year 2000 efforts in the water sector, and little additional information was expected under the current regulatory approach. While the Council's water sector working group had undertaken an awareness campaign and had urged national water sector associations to continue to survey their memberships, survey response rates had been low. Further, Environmental Protection Agency officials stated that the agency lacked the rules and regulations necessary to require water and wastewater facilities to report on their Year 2000 status.

Our survey of state regulators found that a few states were proactively collecting Year 2000 compliance data from regulated facilities, a much larger group of states was disseminating Year 2000 information, while another group was not actively using either approach. Additionally, only a handful of state regulators believed that they were

[58] This was based on the percentage of the total megawatts of the systems reported as Year 2000 ready by investor-owned, public power, and cooperative organizations. The report did not identify the number of local distribution organizations that reported that they were Year 2000 ready.

[59] Year 2000 Computing Crisis: Readiness of the Oil and Gas Industries (GAO/AIMD-99-162, May 19, 1999).

[60] Year 2000 Computing Crisis: Status of the Water Industry (GAO/AIMD-99-151, April 21, 1999).

responsible for ensuring facilities' Year 2000 compliance or overseeing facilities' business continuity and contingency plans. Among our suggested actions was that the Council, the Environmental Protection Agency, and the states determine which regulatory organization should take responsibility for assessing and publicly disclosing the status and outlook of water sector facilities' Year 2000 business continuity and contingency plans. The Environmental Protection Agency generally agreed with our suggestions but one official noted that additional legislation may be needed if the agency is to take responsibility for overseeing facilities' Year 2000 business continuity and contingency plans.

Health Sector

The health sector includes health care providers (such as hospitals and emergency health care services), insurers (such as Medicare and Medicaid), and biomedical equipment. Last month we reported[61] that HCFA had taken aggressive and comprehensive outreach efforts with regard to its over 1.1 million healthcare providers that administer services for Medicare-insured patients.[62] Despite these efforts, HCFA data show that provider participation in its outreach activities has been low. Further, although HCFA has tasked contractors that process Medicare claims with testing with providers using future-dated claims, such testing had been limited and the testing that had occurred had identified problems. Our July report also found that although many surveys had been completed in 1999 on the Year 2000 readiness of healthcare providers; none of the 11 surveys we reviewed provided sufficient information with which to assess the Year 2000 status of the healthcare provider community. Each of the surveys had low response rates, and several did not address critical questions about testing and contingency planning.

To reduce the risk of Year 2000-related failures in the Medicare provider community, our July report suggested, for example, that HCFA consider using additional outreach methods, such as public service announcements, and set milestones for Medicare contractors for testing with providers. We also made suggestions to the President's Council on Year 2000 Conversion's healthcare sector working group, including a suggestion to consider working with associations to publicize those providers who respond to future surveys in order to increase survey response rates. The HCFA Administrator generally agreed with our suggested actions.

With respect to biomedical equipment, on June 10 we testified[63] that, in response to our September 1998 recommendation,[64] HHS, in conjunction with the Department of

[61] Year 2000 Computer Crisis: Status of Medicare Providers Unknown (GAO/AIMD-99-243, July 28, 1999).
[62] Examples of such providers are hospitals, laboratories, physicians, and skilled nursing/long term care facilities.
[63] Year 2000 Computing Challenge: Concerns About Compliance Information on Biomedical Equipment (GAO/T-AIMD-99-209, June 10, 1999).
[64] Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown (GAO/AIMD-98-240, September 18, 1998).

Veterans Affairs, had established a clearinghouse on biomedical equipment. As of June 1, 1999, 4,142 biomedical equipment manufacturers had submitted data to the clearinghouse. About 61 percent of these manufacturers reported having products that do not employ dates and about 8 percent (311 manufacturers) reported having date-related problems such as an incorrect display of date/time. According to the Food and Drug Administration, the 311 manufacturers reported 897 products with date-related problems. However, not all compliance information was available on the clearinghouse because the clearinghouse referred the user to 427 manufacturers' web sites. Accordingly, we reviewed the web sites of these manufacturers and found, as of June 1, 1999, a total of 35,446 products.[65] Of these products, 18,466 were reported as not employing a date, 11,211 were reported as compliant, 4,445 were shown as not compliant, and the compliance status of 1,324 was unknown.

In addition to the establishment of a clearinghouse, our September 1998 report[66] also recommended that HHS and the Department of Veterans Affairs take prudent steps to jointly review manufacturers' test results for critical care/life support biomedical equipment. We were especially concerned that the departments review test results for equipment previously deemed to be noncompliant but now deemed by manufacturers to be compliant, or equipment for which concerns about compliance remained. In May 1999, the Food and Drug Administration, a component agency of HHS, announced that it planned to develop a list of critical care/life support medical devices and the manufacturers of these devices, select a sample of manufacturers for review, and hire a contractor to develop a program to assess manufacturers' activities to identify and correct Year 2000 problems for these medical devices. In addition, if the results of this review indicated a need for further review of manufacturer activities, the contractor would review a portion of the remaining manufacturers not yet reviewed. Moreover, according to the Food and Drug Administration, any manufacturer whose quality assurance system appeared deficient based on the contractors review would be subject to additional reviews to determine what actions would be required to eliminate any risk posed by noncompliant devices.

In April testimony[67] we also reported on the results of a Department of Veterans Affairs survey of 384 pharmaceutical firms and 459 medical-surgical firms with whom it does business. Of the 52 percent of pharmaceutical firms that responded to the survey, 32 percent reported that they were compliant. Of the 54 percent of the medical-surgical firms that responded, about two-thirds reported that they were compliant.

[65] Because of limitations in many of the manufacturers web sites, our ability to determine the total number of biomedical equipment products reported and their compliance status was impaired. Accordingly, the actual number of products reported by the manufacturers could be significantly higher than the 35,446 products that we counted.

[66] GAO/AIMD-98-240, September 18, 1998.

[67] Year 2000 Computing Crisis: Action Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/T-AIMD-99-136, April 15, 1999).

Banking and Finance Sector

A large portion of the institutions that make up the banking and finance sector are overseen by one or more federal regulatory agencies. In September 1998 we testified on the efforts of five federal financial regulatory agencies[68] to ensure that the institutions that they oversee are ready to handle the Year 2000 problem.[69] We concluded that the regulators had made significant progress in assessing the readiness of member institutions and in raising awareness on important issues such as contingency planning and testing. Regulator examinations of bank, thrift, and credit union Year 2000 efforts found that the vast majority were doing a satisfactory job of addressing the problem. Nevertheless, the regulators faced the challenge of ensuring that they are ready to take swift action to address those institutions that falter in the later stages of correction and to address disruptions caused by international and public infrastructure failures.

In April, we reported that the Federal Reserve System--which is instrumental to our nation's economic well-being, since it provides depository institutions and government agencies services such as processing checks and transferring funds and securities, has effective controls to help ensure that its Year 2000 progress is reported accurately and reliably.[70] We also found that it is effectively managing the renovation and testing of its internal systems and the development and planned testing of contingency plans for continuity of business operations. Nevertheless, the Federal Reserve System still had much to accomplish before it is fully ready for January 1, 2000, such as completing validation and implementation of all of its internal systems and completing its contingency plans.

In addition to the domestic banking and finance sector, large U.S. financial institutions have financial exposures and relationships with international financial institutions and markets that may be at risk if these international organizations are not ready for the date change occurring on January 1, 2000. In April, we reported[71] that foreign financial institutions had reportedly lagged behind their U.S. counterparts in preparing for the Year 2000 date change. Officials from four of the seven large foreign financial institutions we visited said they had scheduled completion of their Year 2000 preparations about 3 to 6 months after their U.S. counterparts, but they planned to complete their efforts by mid-1999 at the latest. Moreover, key international market supporters, such as those that transmit financial messages and provide clearing and settlement services, told us that

[68] The National Credit Union Administration, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the Federal Reserve System, and the Office of the Comptroller of the Currency.

[69] Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain (GAO/T-AIMD-98-305, September 17, 1998).

[70] Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Conversion (GAO/AIMD-99-78, April 9, 1999).

[71] Year 2000: Financial Institution and Regulatory Efforts to Address International Risks (GAO/GGD-99-62, April 27, 1999).

their systems were ready for the date change and that they had begun testing with the financial organizations that depended on these systems. Further, we found that seven large U.S. banks and securities firms we visited were taking actions to address their international risks. In addition, U.S. banking and securities regulators were also addressing the international Year 2000 risks of the institutions that they oversee.

With respect to the insurance industry, in March, we concluded that insurance regulator presence regarding the Year 2000 area was not as strong as that exhibited by the banking and securities industry.[72] State insurance regulators we contacted were late in raising industry awareness of potential Year 2000 problems, provided little guidance to regulated institutions, and failed to convey clear regulatory expectations to companies about Year 2000 preparations and milestones. Nevertheless, the insurance industry is reported by both its regulators and by other outside observers to be generally on track to being ready for 2000. However, most of these reports are based on self-reported information and, compared to other financial regulators, insurance regulators' efforts to validate this information generally began late and were more limited.

In a related report in April,[73] we stated that variations in oversight approaches by state insurance regulators also made it difficult to ascertain the overall status of the insurance industry's Year 2000 readiness. We reported that the magnitude of insurers' Year 2000-related liability exposures could not be estimated at that time but that costs associated with these exposures could be substantial for some property-casualty insurers, particularly those concentrated in commercial-market sectors. In addition, despite efforts to mitigate potential exposures, the Year 2000-related costs that may be incurred by insurers would remain uncertain until key legal issues and actions on pending legislation were resolved.

Transportation Sector

A key component to the nation's transportation sector are airports. This January we reported on our survey of 413 airports.[74] We found that while the nation's airports were making progress in preparing for the year 2000, such progress varied. Of the 334 airports responding to our survey, about one-third reported that they would complete their Year 2000 preparations by June 30, 1999. The other two-thirds either planned on a later date or failed to estimate any completion date, and half of these airports did not have contingency plans for any of 14 core airport functions. Although most of those not expecting to be ready by June 30 are small airports, 26 of them are among the nation's largest 50 airports.

[72] Insurance Industry: Regulators Are Less Active in Encouraging and Validating Year 2000 Preparedness (GAO/T-GGD-99-56, March 11, 1999).

[73] Year 2000: State Insurance Regulators Face Challenges in Determining Industry Readiness (GAO/GGD-99-87, April 30, 1999).

[74] Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem (GAO/RCED/AIMD-99-57, January 29, 1999).

International

In addition to the risks associated with the nation's key economic sectors, one of the largest and most uncertain area of risk relates to the global nature of the problem. Table 3 summarizes the results of the Department of State's Office of the Inspector General's analysis of "Y2K Host Country Infrastructure" assessments submitted by U.S. embassies in 161 countries (98 from the developing world, 24 from former Easter bloc countries and the New Independent States, and 39 from industrialized countries). The following table shows that about half of the countries are reported to be at medium or high risk of having Year 2000-related failures in the key areas of telecommunications, transportation, and energy. While a smaller number of countries were reported at medium or high risk in the finance and water sectors, at least one third of the countries fell into the medium or high risk categories.

Table 3: Risk of Year 2000-Related Sector Failures in 161 Countries

Risk Level	Finance	Telecommunications	Transportation	Energy	Water
High	11	35	18	26	7
Medium	43	56	61	64	52
Low	107	70	82	71	102

Source: Year 2000 Computer Problem: Global Readiness and International Trade (Statement of the Department of State's Inspector General before the Senate Special Committee on the Year 2000 Technology Problem, July 22, 1999).

The Department of State Inspector General concluded that the global community is likely to experience varying degrees of Year 2000-related failures—from mere annoyances to failures in key infrastructure systems—in every sector, region, and economic level. In particular, the Inspector General testified on July 22, 1999, that

- Industrialized countries were generally at low risk of having Year 2000-related infrastructure failures although some of these countries were at risk.
- Developing countries were lagging behind and were struggling to find the financial and technical resources needed to resolve their Year 2000 problems.
- Former Eastern bloc countries were late in getting started and were generally unable to provide detailed information on their Year 2000 programs.

The impact of Year 2000-induced failures in foreign countries could adversely affect the United States, particularly as it relates to the supply chain. To address the international supply chain issue, in January 1999 we suggested[75] that the President's Council on Year

[75] GAO/T-AIMD-99-50, January 20, 1999.

2000 Conversion prioritize trade and commerce activities that are critical to the nation's well-being (e.g., oil, food, pharmaceuticals) and, working with the private sector, identify options for obtaining these materials through alternative avenues in the event that Year 2000-induced failures in the other country or in the transportation sector prevent these items from reaching the United States. In commenting on this suggestion, the Chair stated that the Council had (1) worked with federal agencies to identify sectors with the greatest dependence on international trade, (2) held industry roundtable discussions with the pharmaceutical and food supply sectors, and (3) hosted bilateral and trilateral meetings with the Council's counterparts in Canada and Mexico—the United States' largest trading partners.

- - - - -

In summary, while improvement has been shown, much work remains at the national, federal, state, and local levels to ensure that major service disruptions do not occur. Specifically, remediation must be completed, end-to-end testing performed, and business continuity and contingency plans developed. Similar actions remain to be completed by the nation's key sectors. Accordingly, whether the United States successfully confronts the Year 2000 challenge will largely depend on the success of federal, state, and local governments, as well as the private sector working separately and together to complete these actions. Accordingly, strong leadership and partnerships must be maintained to ensure that the needs of the public are met at the turn of the century.

Mr. Chairman, this concludes my statement. I would be happy to respond to any questions that you or other members of the Subcommittee may have at this time.

Contacts

For information concerning this testimony, please contact Joel Willemssen at (202) 512-6253 or by e-mail at willemssenj.aimd@gao.gov.

Federal High-Impact Programs and Lead Agencies

Agency	Program
Department of Agriculture	Child Nutrition Programs
Department of Agriculture	Food Safety Inspection
Department of Agriculture	Food Stamps
Department of Agriculture	Special Supplemental Nutrition Program for Women, Infants, and Children
Department of Commerce	Patent and trademark processing
Department of Commerce	Weather Service
Department of Defense	Military Hospitals
Department of Defense	Military Retirement
Department of Education	Student Aid
Department of Energy	Federal electric power generation and delivery
Department of Health and Human Services	Child Care
Department of Health and Human Services	Child Support Enforcement
Department of Health and Human Services	Child Welfare
Department of Health and Human Services	Disease monitoring and the ability to issue warnings
Department of Health and Human Services	Indian Health Service
Department of Health and Human Services	Low Income Home Energy Assistance Program
Department of Health and Human Services	Medicaid
Department of Health and Human Services	Medicare
Department of Health and Human Services	Organ Transplants
Department of Health and Human Services	Temporary Assistance for Needy Families
Department of Housing and Urban Development	Housing loans (Government National Mortgage Association)

Department of Housing and Urban Development	Section 8 Rental Assistance
Department of Housing and Urban Development	Public Housing
Department of Housing and Urban Development	FHA Mortgage Insurance
Department of Housing and Urban Development	Community Development Block Grants
Department of the Interior	Bureau of Indians Affairs programs
Department of Justice	Federal Prisons
Department of Justice	Immigration
Department of Justice	National Crime Information Center
Department of Labor	Unemployment Insurance
Department of State	Passport Applications and Processing
Department of Transportation	Air Traffic Control System
Department of Transportation	Maritime Safety Program
Department of the Treasury	Cross-border Inspection Services
Department of Veterans Affairs	Veterans' Benefits
Department of Veterans Affairs	Veterans' Health Care
Federal Emergency Management Agency	Disaster Relief
Office of Personnel Management	Federal Employee Health Benefits
Office of Personnel Management	Federal Employee Life Insurance
Office of Personnel Management	Federal Employee Retirement Benefits
Railroad Retirement Board	Retired Rail Workers Benefits
Social Security Administration	Social Security Benefits
U.S. Postal Service	Mail Service

GAO REPORTS AND TESTIMONY ADDRESSING THE YEAR 2000 CRISIS

Year 2000 Computing Challenge: Agencies' Reporting of Mission-Critical Classified Systems (GAO/AIMD-99-218, August 5, 1999)

Social Security Administration: Update on Year 2000 and Other Key Information Technology Initiatives (GAO/T-AIMD-99-259, July 29, 1999)

Year 2000 Computing Crisis: Status of Medicare Providers Unknown (GAO/AIMD-99-243, July 28, 1999)

Reported Y2K status of the 21 Largest U.S. Cities (GAO/AIMD-99-246R, July 15, 1999)

Year 2000 Computing Challenge: Federal Efforts to Ensure Continued Delivery of Key State-Administered Benefits (GAO/T-AIMD-99-241, July 15, 1999)

Emergency and State and Local Law Enforcement Systems: Committee Questions Concerning Year 2000 Challenges (GAO/AIMD-99-247R, July 14, 1999)

Year 2000 Computing Challenge: Important Progress Made, Yet Much Work Remains to Avoid Disruption of Critical Services (GAO/T-AIMD-99-234, July 9, 1999)

Year 2000 Computing Challenge: Readiness Improving Yet Avoiding Disruption of Critical Services Will Require Additional Work (GAO/T-AIMD-99-233, July 8, 1999)

Year 2000 Computing Challenge: Readiness Improving But Much Work Remains to Avoid Disruption of Critical Services (GAO/T-AIMD-99-232, July 7, 1999)

Defense Computers: Management Controls Are Critical To Effective Year 2000 Testing (GAO/AIMD-99-172, June 30, 1999)

Year 2000 Computing Crisis: Customs is Making Good Progress (GAO/T-AIMD-99-225, June 29, 1999)

Year 2000 Computing Challenge: Delivery of Key Benefits Hinges on States' Achieving Compliance (GAO/T-AIMD/GGD-99-221, June 23, 1999)

Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications (GAO/T-AIMD-99-214, June 22, 1999).

GSA's Effort to Develop Year 2000 Business Continuity and Contingency Plans for Telecommunications Systems (GAO/AIMD-99-201R, June 16, 1999).

Year 2000 Computing Crisis: Actions Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/AIMD-99-190R, June 11, 1999)

Year 2000 Computing Challenge: Concerns About Compliance Information on Biomedical Equipment (GAO/T-AIMD-99-209, June 10, 1999)

Year 2000 Computing Challenge: Much Biomedical Equipment Status Information Available, Yet Concerns Remain (GAO/T-AIMD-99-197, May 25, 1999)

Year 2000 Computing Challenge: OPM Has Made Progress on Business Continuity Planning (GAO/GGD-99-66, May 24, 1999)

VA Y2K Challenges: Responses to Post-Testimony Questions (GAO/AIMD-99-199R, May 24, 1999)

Year 2000 Computing Crisis: USDA Needs to Accelerate Time Frames for Completing Contingency Planning (GAO/AIMD-99-178, May 21, 1999)

Year 2000 Computing Crisis: Readiness of the Oil and Gas Industries (GAO/AIMD-99-162, May 19, 1999)

Year 2000 Computing Challenge: Time Issues Affecting the Global Positioning System (GAO/T-AIMD-99-187, May 12, 1999)

Year 2000 Computing Challenge: Education Taking Needed Actions But Work Remains (GAO/T-AIMD-99-180, May 12, 1999)

Year 2000 Computing Challenge: Labor Has Progressed But Selected Systems Remain at Risk (GAO/T-AIMD-99-179, May 12, 1999)

Year 2000: State Insurance Regulators Face Challenges in Determining Industry Readiness (GAO/GGD-99-87, April 30, 1999)

Year 2000 Computing Challenge: Status of Emergency and State and Local Law Enforcement Systems Is Still Unknown (GAO/T-AIMD-99-163, April 29, 1999)

Year 2000 Computing Crisis: Costs and Planned Use of Emergency Funds (GAO/AIMD-99-154, April 28, 1999)

Year 2000: Financial Institution and Regulatory Efforts to Address International Risks (GAO/GGD-99-62, April 27, 1999)

Year 2000 Computing Crisis: Readiness of Medicare and the Health Care Sector (GAO/T-AIMD-99-160, April 27, 1999)

U.S. Postal Service: Subcommittee Questions Concerning Year 2000 Challenges Facing the Service (GAO/AIMD-99-150R, April 23, 1999)

Year 2000 Computing Crisis: Status of the Water Industry (GAO/AIMD-99-151, April 21, 1999)

Year 2000 Computing Crisis: Key Actions Remain to Ensure Delivery of Veterans Benefits and Health Services (GAO/T-AIMD-99-152, April 20, 1999)

Year 2000 Computing Crisis: Readiness Improving But Much Work Remains To Ensure Delivery of Critical Services (GAO/T-AIMD-99-149, April 19, 1999)

Year 2000 Computing Crisis: Action Needed to Ensure Continued Delivery of Veterans Benefits and Health Care Services (GAO/T-AIMD-99-136, April 15, 1999)

Year 2000 Computing Challenge: Federal Government Making Progress But Critical Issues Must Still Be Addressed to Minimize Disruptions (GAO/T-AIMD-99-144, April 14, 1999)

Year 2000 Computing Crisis: Additional Work Remains to Ensure Delivery of Critical Services (GAO/T-AIMD-99-143, April 13, 1999)

Tax Administration: IRS' Fiscal Year 2000 Budget Request and 1999 Tax Filing Season (GAO/T-GGD/AIMD-99-140, April 13, 1999).

Year 2000 Computing Crisis: Federal Reserve Has Established Effective Year 2000 Management Controls for Internal Systems Conversion (GAO/AIMD-99-78, April 9, 1999)

Year 2000 Computing Crisis: Readiness of the Electric Power Industry (GAO/AIMD-99-114, April 6, 1999)

Year 2000 Computing Crisis: Customs Has Established Effective Year 2000 Program Controls (GAO/AIMD-99-37, March 29, 1999)

Year 2000 Computing Crisis: FAA Is Making Progress But Important Challenges Remain (GAO/T-AIMD/RCED-99-118, March 15, 1999)

Insurance Industry: Regulators Are Less Active in Encouraging and Validating Year 2000 Preparedness (GAO/T-GGD-99-56, March 11, 1999)

Year 2000 Computing Crisis: Defense Has Made Progress, But Additional Management Controls Are Needed (GAO/T-AIMD-99-101, March 2, 1999)

Year 2000 Computing Crisis: Readiness Status of the Department of Health and Human Services (GAO/T-AIMD-99-92, February 26, 1999)

Defense Information Management: Continuing Implementation Challenges Highlight the Need for Improvement (GAO/T-AIMD-99-93, February 25, 1999)

IRS' Year 2000 Efforts: Status and Remaining Challenges (GAO/T-GGD-99-35, February 24, 1999)

Department of Commerce: National Weather Service Modernization and NOAA Fleet Issues (GAO/T-AIMD/GGD-99-97, February 24, 1999)

Year 2000 Computing Crisis: Medicare and the Delivery of Health Services Are at Risk (GAO/T-AIMD-99-89, February 24, 1999)

Year 2000 Computing Crisis: Readiness of State Automated Systems That Support Federal Human Services Programs (GAO/T-AIMD-99-91, February 24, 1999)

Year 2000 Computing Crisis: Customs Is Effectively Managing Its Year 2000 Program (GAO/T-AIMD-99-85, February 24, 1999)

Year 2000 Computing Crisis: Update on the Readiness of the Social Security Administration (GAO/T-AIMD-99-90, February 24, 1999)

Year 2000 Computing Crisis: Challenges Still Facing the U.S. Postal Service (GAO/T-AIMD-99-86, February 23, 1999)

Year 2000 Computing Crisis: The District of Columbia Remains Behind Schedule (GAO/T-AIMD-99-84, February 19, 1999)

High-Risk Series: An Update (GAO/HR-99-1, January 1999)

Year 2000 Computing Crisis: Status of Airports' Efforts to Deal With Date Change Problem (GAO/RCED/AIMD-99-57, January 29, 1999)

Defense Computers: DOD's Plan for Execution of Simulated Year 2000 Exercises (GAO/AIMD-99-52R, January 29, 1999)

Year 2000 Computing Crisis: Status of Bureau of Prisons' Year 2000 Efforts (GAO/AIMD-99-23, January 27, 1999)

Year 2000 Computing Crisis: Readiness Improving, But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, January 20, 1999)

Year 2000 Computing Challenge: Readiness Improving, But Critical Risks Remain (GAO/T-AIMD-99-49, January 20, 1999)

Status Information: FAA's Year 2000 Business Continuity and Contingency Planning Efforts Are Ongoing (GAO/AIMD-99-40R, December 4, 1998)

Year 2000 Computing Crisis: A Testing Guide (GAO/AIMD-10.1.21, November 1998)

Year 2000 Computing Crisis: Readiness of State Automated Systems to Support Federal Welfare Programs (GAO/AIMD-99-28, November 6, 1998)

Year 2000 Computing Crisis: Status of Efforts to Deal With Personnel Issues (GAO/AIMD/GGD-99-14, October 22, 1998)

Year 2000 Computing Crisis: Updated Status of Department of Education's Information Systems (GAO/T-AIMD-99-8, October 8, 1998)

Year 2000 Computing Crisis: The District of Columbia Faces Tremendous Challenges in Ensuring That Vital Services Are Not Disrupted (GAO/T-AIMD-99-4, October 2, 1998)

Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy (GAO/AIMD-98-284, September 28, 1998)

Year 2000 Computing Crisis: Leadership Needed to Collect and Disseminate Critical Biomedical Equipment Information (GAO/T-AIMD-98-310, September 24, 1998)

Year 2000 Computing Crisis: Compliance Status of Many Biomedical Equipment Items Still Unknown (GAO/AIMD-98-240, September 18, 1998)

Year 2000 Computing Crisis: Significant Risks Remain to Department of Education's Student Financial Aid Systems (GAO/T-AIMD-98-302, September 17, 1998)

Year 2000 Computing Crisis: Progress Made at Department of Labor, But Key Systems at Risk (GAO/T-AIMD-98-303, September 17, 1998)

Year 2000 Computing Crisis: Federal Depository Institution Regulators Are Making Progress, But Challenges Remain (GAO/T-AIMD-98-305, September 17, 1998)

Year 2000 Computing Crisis: Federal Reserve Is Acting to Ensure Financial Institutions Are Fixing Systems But Challenges Remain (GAO/AIMD-98-248, September 17, 1998)

Responses to Questions on FAA's Computer Security and Year 2000 Program (GAO/AIMD-98-301R, September 14, 1998)

Year 2000 Computing Crisis: Severity of Problem Calls for Strong Leadership and Effective Partnerships (GAO/T-AIMD-98-278, September 3, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Partnerships Needed to Reduce Likelihood of Adverse Impact (GAO/T-AIMD-98-277, September 2, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Partnerships Needed to Mitigate Risks (GAO/T-AIMD-98-276, September 1, 1998)

Year 2000 Computing Crisis: State Department Needs To Make Fundamental Improvements To Its Year 2000 Program (GAO/AIMD-98-162, August 28, 1998)

Year 2000 Computing: EFT 99 Is Not Expected to Affect Year 2000 Remediation Efforts (GAO/AIMD-98-272R, August 28, 1998)

Year 2000 Computing Crisis: Progress Made in Compliance of VA Systems, But Concerns Remain (GAO/AIMD-98-237, August 21, 1998)

Year 2000 Computing Crisis: Avoiding Major Disruptions Will Require Strong Leadership and Effective Partnerships (GAO/T-AIMD-98-267, August 19, 1998)

Year 2000 Computing Crisis: Strong Leadership and Partnerships Needed to Address Risk of Major Disruptions (GAO/T-AIMD-98-266, August 17, 1998)

Year 2000 Computing Crisis: Strong Leadership and Partnerships Needed to Mitigate Risk of Major Disruptions (GAO/T-AIMD-98-262, August 13, 1998)

FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998)

Year 2000 Computing Crisis: Business Continuity and Contingency Planning (GAO/AIMD-10.1.19, August 1998)

Internal Revenue Service: Impact of the IRS Restructuring and Reform Act on Year 2000 Efforts (GAO/GGD-98-158R, August 4, 1998)

Social Security Administration: Subcommittee Questions Concerning Information Technology Challenges Facing the Commissioner (GAO/AIMD-98-235R, July 10, 1998)

Year 2000 Computing Crisis: Actions Needed on Electronic Data Exchanges (GAO/AIMD-98-124, July 1, 1998)

Defense Computers: Year 2000 Computer Problems Put Navy Operations At Risk (GAO/AIMD-98-150, June 30, 1998)

Year 2000 Computing Crisis: Testing and Other Challenges Confronting Federal Agencies (GAO/T-AIMD-98-218, June 22, 1998)

Year 2000 Computing Crisis: Telecommunications Readiness Critical, Yet Overall Status Largely Unknown (GAO/T-AIMD-98-212, June 16, 1998)

GAO Views on Year 2000 Testing Metrics (GAO/AIMD-98-217R, June 16, 1998)

IRS' Year 2000 Efforts: Business Continuity Planning Needed for Potential Year 2000 System Failures (GAO/GGD-98-138, June 15, 1998)

Year 2000 Computing Crisis: Actions Must Be Taken Now to Address Slow Pace of Federal Progress (GAO/T-AIMD-98-205, June 10, 1998)

Defense Computers: Army Needs to Greatly Strengthen Its Year 2000 Program (GAO/AIMD-98-53, May 29, 1998)

Year 2000 Computing Crisis: USDA Faces Tremendous Challenges in Ensuring That Vital Public Services Are Not Disrupted (GAO/T-AIMD-98-167, May 14, 1998)

Securities Pricing: Actions Needed for Conversion to Decimals (GAO/T-GGD-98-121, May 8, 1998)

Year 2000 Computing Crisis: Continuing Risks of Disruption to Social Security, Medicare, and Treasury Programs (GAO/T-AIMD-98-161, May 7, 1998)

IRS' Year 2000 Efforts: Status and Risks (GAO/T-GGD-98-123, May 7, 1998)

Air Traffic Control: FAA Plans to Replace Its Host Computer System Because Future Availability Cannot Be Assured (GAO/AIMD-98-138R, May 1, 1998)

Year 2000 Computing Crisis: Potential For Widespread Disruption Calls For Strong Leadership and Partnerships (GAO/AIMD-98-85, April 30, 1998)

Defense Computers: Year 2000 Computer Problems Threaten DOD Operations (GAO/AIMD-98-72, April 30, 1998)

Department of the Interior: Year 2000 Computing Crisis Presents Risk of Disruption to Key Operations (GAO/T-AIMD-98-149, April 22, 1998)

Tax Administration: IRS' Fiscal Year 1999 Budget Request and Fiscal Year 1998 Filing Season (GAO/T-GGD/AIMD-98-114, March 31, 1998)

Year 2000 Computing Crisis: Strong Leadership Needed to Avoid Disruption of Essential Services (GAO/T-AIMD-98-117, March 24, 1998)

Year 2000 Computing Crisis: Federal Regulatory Efforts to Ensure Financial Institution Systems Are Year 2000 Compliant (GAO/T-AIMD-98-116, March 24, 1998)

Year 2000 Computing Crisis: Office of Thrift Supervision's Efforts to Ensure Thrift Systems Are Year 2000 Compliant (GAO/T-AIMD-98-102, March 18, 1998)

Year 2000 Computing Crisis: Strong Leadership and Effective Public/Private Cooperation Needed to Avoid Major Disruptions (GAO/T-AIMD-98-101, March 18, 1998)

Post-Hearing Questions on the Federal Deposit Insurance Corporation's Year 2000 (Y2K) Preparedness (AIMD-98-108R, March 18, 1998)

SEC Year 2000 Report: Future Reports Could Provide More Detailed Information (GAO/GGD/AIMD-98-51, March 6, 1998)

Year 2000 Readiness: NRC's Proposed Approach Regarding Nuclear Powerplants (GAO/AIMD-98-90R, March 6, 1998)

Yėar 2000 Computing Crisis: Federal Deposit Insurance Corporation's Efforts to Ensure Bank Systems Are Year 2000 Compliant (GAO/T-AIMD-98-73, February 10, 1998)

Year 2000 Computing Crisis: FAA Must Act Quickly to Prevent Systems Failures (GAO/T-AIMD-98-63, February 4, 1998)

FAA Computer Systems: Limited Progress on Year 2000 Issue Increases Risk Dramatically (GAO/AIMD-98-45, January 30, 1998)

Defense Computers: Air Force Needs to Strengthen Year 2000 Oversight (GAO/AIMD-98-35, January 16, 1998)

Year 2000 Computing Crisis: Actions Needed to Address Credit Union Systems' Year 2000 Problem (GAO/AIMD-98-48, January 7, 1998)

Veterans Health Administration Facility Systems: Some Progress Made In Ensuring Year 2000 Compliance, But Challenges Remain (GAO/AIMD-98-31R, November 7, 1997)

Year 2000 Computing Crisis: National Credit Union Administration's Efforts to Ensure Credit Union Systems Are Year 2000 Compliant (GAO/T-AIMD-98-20, October 22, 1997)

Social Security Administration: Significant Progress Made in Year 2000 Effort, But Key Risks Remain (GAO/AIMD-98-6, October 22, 1997)

Defense Computers: Technical Support Is Key to Naval Supply Year 2000 Success (GAO/AIMD-98-7R, October 21, 1997)

Defense Computers: LSSC Needs to Confront Significant Year 2000 Issues (GAO/AIMD-97-149, September 26, 1997)

Veterans Affairs Computer Systems: Action Underway Yet Much Work Remains To Resolve Year 2000 Crisis (GAO/T-AIMD-97-174, September 25, 1997)

Year 2000 Computing Crisis: Success Depends Upon Strong Management and Structured Approach, (GAO/T-AIMD-97-173, September 25, 1997)

Year 2000 Computing Crisis: An Assessment Guide (GAO/AIMD-10.1.14, September 1997)

Defense Computers: SSG Needs to Sustain Year 2000 Progress (GAO/AIMD-97-120R, August 19, 1997)

Defense Computers: Improvements to DOD Systems Inventory Needed for Year 2000 Effort (GAO/AIMD-97-112, August 13, 1997)

Defense Computers: Issues Confronting DLA in Addressing Year 2000 Problems (GAO/AIMD-97-106, August 12, 1997)

Defense Computers: DFAS Faces Challenges in Solving the Year 2000 Problem (GAO/AIMD-97-117, August 11, 1997)

Year 2000 Computing Crisis: Time is Running Out for Federal Agencies to Prepare for the New Millennium (GAO/T-AIMD-97-129, July 10, 1997)

Veterans Benefits Computer Systems: Uninterrupted Delivery of Benefits Depends on Timely Correction of Year-2000 Problems (GAO/T-AIMD-97-114, June 26, 1997)

Veterans Benefits Computer Systems: Risks of VBA's Year-2000 Efforts (GAO/AIMD-97-79, May 30, 1997)

Medicare Transaction System: Success Depends Upon Correcting Critical Managerial and Technical Weaknesses (GAO/AIMD-97-78, May 16, 1997)

Medicare Transaction System: Serious Managerial and Technical Weaknesses Threaten Modernization (GAO/T-AIMD-97-91, May 16, 1997)

Year 2000 Computing Crisis: Risk of Serious Disruption to Essential Government Functions Calls for Agency Action Now (GAO/T-AIMD-97-52, February 27, 1997)

Year 2000 Computing Crisis: Strong Leadership Today Needed To Prevent Future Disruption of Government Services (GAO/T-AIMD-97-51, February 24, 1997)

High-Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997)

(511790)

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

http://www.gao.gov

PRINTED ON ♻ RECYCLED PAPER

Mr. HORN. Thank you very much. Our next witness is Chris Hedrick. He is the director for the State Year 2000 Office for the State of Washington. Mr. Hedrick.

Mr. HEDRICK. Thank you very much, Mr. Chairman, Congressman McDermott, Congresswoman Dunn. I appreciate the invitation to testify before the committee.

Washington State government is a complex organization. We've got 39 major agencies with over 400 mission-critical computer systems and 43 agencies with embedded chips in systems that support vital public services and a higher education system that's very broad.

As long ago as 1993, State agencies recognized the challenge and began working on this issue. In 1995, the State Department of Information Services established a central program to get computer data systems for State agencies and higher educational institutions ready for the date transition.

We've adopted a phased approach: conducted inventories, identified the resources needed to correct the problems, and, in cases, asked the State legislature for those resources, conducted pilot projects, and actually converted the systems. All along, we've had independent assessments of our progress, outside auditing, and rigorous testing. All State agencies have also established and completed contingency plans in case vital public services are interrupted by other factors.

In 1997, Governor Locke established two goals for State government's Y2K efforts: no interruption of vital public services, and no loss of accountability for public resources. We've spent over $80 million trying to achieve those goals, and we've made some progress.

Risk assessment and independent auditing have been really key to our efforts. Here's how the process works. The State agencies have contracted with independent risk assessors who evaluate all the mission-critical computer systems and embedded systems. Then another contractor compiles this assessment data, analyzes it through a standardized process, and issues regular progress reports, such as this one.

This contractor gives us a report card based on our progress. We get either red, yellow, or green ratings, or blue if the system is certified. As you can see from this page, our most recent report is all blue and green. Over 98 percent of State government computer systems are now fully compliant.

The important part about this independent risk assessment is that the information is released to the cabinet with the governor in his regular cabinet meetings and to the press on the same day, and we've found that to be a powerful management tool.

As I said, over 98 percent of our mission-critical data systems have satisfactorily completed the test for Y2K compliance. Those few programs that are not done will be completed over the next several weeks. And all computer systems in State agencies and higher educational institutions have established contingency plans. We have adopted the General Accounting Office standards for contingency planning, and those have been very useful in our efforts.

We've had some initial successes. In January of this year, our unemployment claims system made a successful transition. That system looks forward a year for eligibility benefits. Last month, our State financial systems had a successful transition to fiscal year 2000. And these successful efforts give us increasing confidence in our ability to deal with the calendar year change next January.

But in addition to our efforts to take care of our own computer systems and ensure that they'll make the transition successfully, we've taken on the responsibility of providing the public with information and an array of tools to ensure their own preparedness. We've conducted a series of workshops across the State, both for the public, for small businesses, and for local governments.

We've been very aggressive about our use of the Internet in providing public information. In fact, we're building a system where every individual citizen can go to our website and pull down their own personalized profile with information about the readiness status of each local government, electricity, natural gas providers——

Mr. HORN. Let me suggest—I'm an expert now on microphones—you need to get that pointed very close to you, otherwise they won't hear you in the back of the room.

Mr. HEDRICK. Thank you. Readiness status of local governments, electricity, natural gas providers, financial institutions and government benefit programs.

Underlying all of our work in public information is our belief that people make good choices if they have good information. And we think it is our responsibility not to sugar coat that information, but to provide the public with the best information available.

In assembling that information, we have also provided, both in print and on the web, two volumes of the Washington State Year 2000 Readiness Report. The third volume will come out in November. These reports are written with the help of staff from various State agencies, from local governments, and from our private sector advisory group, which includes representatives of all the major industries.

They include information about the Y2K preparedness in Washington State of a variety of sectors, including local and State government, electricity, telecommunications, financial services, natural gas and petroleum, water supply and treatment, emergency management, health care, environmental quality programs, insurance, food supply, public safety, and transportation.

We believe that we've been pretty responsible about making our house in order, but we also believe it's our responsibility to ensure that the citizens of Washington State have a pretty good idea of how messy or clean the Y2K house is for the rest of the State.

In that effort, Mr. Chairman, at the State level, we share your national goal, and we appreciate what you've been doing on the Federal level. Thank you for the opportunity to testify. I'll be happy to take questions at the conclusion.

Mr. HORN. We'll do it when all the panel has participated.

Let me say that we will take questions from the audience written out on a card. And staff will be going up and down each side, and if you have paper—I think staff have the paper and the index cards—please feel free to write them out, and then we will put those questions that you have into the dialog at the end of this panel.

And so let us now go to Mr. Clif Burwell, the Y2K program manager for King County. Thank you for coming, Mr. Burwell.

[The prepared statement of Mr. Hedrick follows:]

Testimony of Christopher Hedrick

Technology Policy Advisor to Governor Locke
and Director of the Washington State Year 2000 Office

www.wa.gov/2000

August 17, 1999

Thank you for the invitation to testify before your committee. Today, I would like to touch upon the readiness of Washington State government for the Year 2000 transition and our strategies for communications on the issue

Washington State government operates a complex array of computer systems and facilities, including:

- 39 major agencies with a combined total of 432 mission-critical computer data systems
- 43 agencies with embedded chips in systems that support vital public services
- 7 major data centers, and
- 2 major backbone networks

As long as ago as 1993, state agencies recognized the challenge and began working to identify and solve potential problems. In 1995, the Department of Information Services established a central program to get state computer data systems ready for the Year 2000, coordinating efforts among various state agencies.

In a phased approach, state agencies:

- Conducted inventories to identify the scope of the potential problem
- Set specific goals for addressing the problem
- Identified the resources needed to correct the problem at a reasonable cost
- Conducted pilot projects
- Began converting systems
- Initiated independent assessments of risks for mission-critical systems and vital public services
- Began testing updated systems, and
- Established contingency plans in case vital public services are interrupted

In 1997, Governor Locke established two goals for state government's Year 2000 efforts: no interruption of vital public services and no loss of accountability for public resources. Since then, the state legislature has allocated over $80 million specifically to address the Y2K transition.

Washington State government has made it a priority to provide updated and reliable information, obtained independently, for decision-making about Year 2000 corrective actions. To ensure objectivity, the state contracted with Sterling Associates, a technology consulting firm, to coordinate statewide Year 2000 risk assessment reports for computer systems through the Department of Information Systems. The state also contracted with Sterling to coordinate risk assessment reports for embedded chips in facilities and equipment, as well as agencies' contingency planning. Washington was one of the first states in the nation to contract for independent assessments.

Here's how the risk assessment process works:

- State agencies have contracted with independent risk management consultants who evaluate all mission-critical computer systems and vital public services projects.
- Another independent contractor, Sterling Associates, compiles this assessment data, analyzes it through a standardized process, and issues regular progress reports. These reports identify state government mission-critical systems and vital services in one of these categories: high risk of interruption, moderate risk, low risk, or certified as Y2K-compliant.
- This information is reviewed with the Governor and Executive Cabinet members, who monitor state agencies' and institutions' progress on having state systems, equipment and facilities ready by the state's June 30, 1999, target date for Y2K completion. It is released to the press and the public the same day that it is presented to the cabinet. We have found this transparency and independent assessment to be a powerful management tool.

As of this week, 98 percent of Washington State government's mission-critical computer data systems had satisfactorily completed tests for Y2K compliance. Those few programs that are not complete all have tested contingency plans in place to deal with any potential malfunctions. As of July 30, 69 percent of the 84 projects to test and fix embedded computer systems—82 percent--we complete and all but one has been assessed as a low risk of experiencing failures.

State agencies are required to develop Year 2000 contingency plans if they have mission-critical computer systems or vital public services that are at risk of interruption due to internal factors such as computer data systems or embedded microchips, or external factors such as power disruption. State government's Year 2000 Executive Steering Committee has adopted the "General Accounting Office, Year 2000 Business Continuity and Contingency Planning" document as the standard of practice for agency contingency planning.

A risk of disruption, therefore, doesn't mean the service will be shut down. Instead, alternative modes of delivery are identified and tested. For example, if a vendor payment system relies on a particular computer application, the affected agency would put a backup system into place, such as a manual payment system. This backup system would operate until the original computer application is brought back into service.

All agency contingency plans have now been completed and are an essential factor in enabling agencies to achieve the governor's goal of no interruption of vital public services and no loss of accountability for public resources.

We have had some initial successes with our efforts. This January our unemployment insurance computer systems made a flawless transition to the Year 2000. These systems needed to be fixed early since the unemployment benefits calculation looks forward one year. Last month, our state financial systems we made a successful transition to our Fiscal Year 2000. These successful efforts give us increasing confidence in our ability to deal with the calendar year change next January.

In addition to our efforts to take care of our own computer systems and ensure that they will make the date transition without a hitch, we have taken on the responsibility of providing the public with an array of tools to ensure their own preparedness.

We have aimed for high standards in making Year 2000 technology transition information available to the public. With the help of the Association of Washington Cities and many local co-sponsors, we conducted community and small-business Y2K preparedness workshops in nine cities across the state this spring.

We also posted unique information tools on Washington State's "Year 2000 and You" website. This site allows Washington residents to prepare their own personalized Y2K profile on the web, with information about the readiness status of each local government, electricity and natural gas providers, financial institution, and government benefit programs.

We believe that people make good choices when they have good information. This principle underlies all of our public information efforts.

Commenting on our work, John Koskinen, Chairman of the President's Council on Year 2000 Conversion, said:

> "Washington State is not only doing an excellent job in getting its systems ready for the Year 2000, it has been a leader in providing credible and useful information to its citizens in innovative ways. I congratulate the state for all of its hard work on the Y2K problem."

This year, we have published, both in print and on the web, two volumes of the Washington State Year 2000 Readiness Report. These reports were written with the help of staff at numerous state agencies, local governments and from our private sector advisory board, which includes representatives of all the major industries that people depend upon.

These reports have included information about Y2K preparedness of a variety of service sectors: local and state government, electricity, telecommunications, financial services, natural gas and petroleum, water supply and treatment, emergency management, , health care, environmental quality programs, insurance, food supply, public safety, and air, marine and land transportation. In November, we will publish Volume 3 of the Washington State Year 2000 Readiness Report.

We believe that we have been very responsible about making our house in order. We want to make sure that the public has the best information possible about how clean or messy everyone else's Y2K house is in Washington state. In that effort, at the state level we share your national goal, Mr. Chairman.

Thank you for the opportunity to testify. I would be delighted to take any questions at this time.

Mr. BURWELL. Thank you very much, Chairman Horn, Congresswoman Dunn, Congressman McDermott. Can you hear me?

Mr. HORN. You'll have to talk into that microphone or you won't be heard past your colleague to the left.

Mr. BURWELL. OK. I'm very happy to be here on behalf of King County. I'm wondering if I would be in trouble if I admitted that I was one of those programmers in 1967 that you mentioned that was compressing those dates. I think now I'm having payback now by being——

Mr. HORN. Were you using COBOL?

Mr. BURWELL. We were using COBOL.

Mr. HORN. Well, I actually made a little program in COBOL, not as many as the two of you. But I must say, they are suddenly gaining justice. The Federal Government has permitted anybody that knows anything about COBOL—they'll still get their Federal pension check, and they can sign a $100,000 contract to solve the problem.

Ms. DUNN. Now we'll get a little credit there. We get to earn a few paychecks by restoring the problem that we created.

Mr. HORN. Right.

Mr. BURWELL. King County took this problem very serious in 1996, and the Council initiated a proviso. The executive supported that proviso in establishing the Y2K Program Office. And we started our work in three phases. Phase I was the mainframe/centralized system, which King County, at that time, had a lot of systems. Then we moved to the agency systems. And then the third phase is the independent audit and certification.

Our project overall is—King County now is 88 percent complete at this time, with most mission-critical systems being done. The systems that aren't done are primarily vendor systems that had to be replaced because they were not compliant.

Our project was organized by business area, and I'd like to quickly go through that. The four business areas that we're addressing are law, safety, and justice, general government, transportation and land use, and health and human services.

In the area of law, safety, and justice, basic police services in King County are Y2K-ready. The E–911 system within King County is Y2K-ready. Criminal investigation, fingerprint identification, special operations, et cetera, all within the public safety area, are ready. Our fingerprint system is being replaced, and that will be implemented in October. Prosecuting attorney systems are ready. Superior court systems, ready.

Adult detention and youth detention systems are ready. In the youth services area, we had one system that had to be replaced, a major system, and that is scheduled for October. All of our infrastructure systems, wide-area network, those kind of systems, have been tested and audited and are ready.

Our 800-MHz communication system which interfaces throughout the region is ready. I mentioned the E–911 system for King County is ready. We're monitoring several public safety answering points in the region as far as their progress, and all 911 systems supported by our system with U.S. West will be ready in September.

Our elections management systems, animal regulation systems, finance systems, construction systems, ready.

One of our challenges has been in the transportation area with transit. The transit division is heavily laden with computer systems, and we've made excellent progress in that area, and expect to have everything ready by September.

An important part of our program is working with the community, and we've done that through what we've called a stakeholders committee, involving both the private sector and the public sector. And we operate this committee through our Emergency Operations Center. Members of that committee include the State, Boeing, Banking Association, city of Seattle, Weyerhaeuser, and several other agencies.

The objective of that committee is to really do the outreach program so that we can communicate and educate not only the other jurisdictions, but the citizens and our employees.

So overall, King County is 88 percent ready with mission-critical systems, and we expect to be ready no later than October. And again, I would be happy to answer any questions at the appropriate time. Thank you.

[The prepared statement of Mr. Burwell follows:]

King County Washington Year 2000 Readiness Status
Presented to U.S. House of Representatives
Committee on Government Reform
Subcommittee on Government Management, Information, and Technology
August 17, 1999 in Seattle

Presented by: Clif Burwell, King County Y2K Program Manager

King County is the largest populated county in the State of Washington. Its population is 1,665,800 and includes the greater Seattle area. There are 2,134 square miles and a density population of 780.6 per square mile. King County provides vital services in the areas of: Law, Safety and Justice; Health and Human Services; Transportation and Land Use Planning; and General Government. There are approximately 11,000 county employees.

In 1996, the Information and Telecommunications Services Division (ITS) of the Department of Information and Administrative Services (DIAS) initiated the Year 2000 project for King County. At that time, planning was initiated to address all hardware, software and applications from the desktop to the County's enterprise mainframe computer. In recognition of the need to ensure that county information is not compromised by the pending year 2000 problem, the King County Council established a legislative proviso that all mission critical systems enterprise-wide be converted and ready no later than April 1999.

The King County Executive supported the proviso by requesting that all agencies develop plans for conversion of agency systems within the 1999 target. A Y2K Program Office was organized to:

1. Provide overall project management;
2. Assist all county agencies in managing Y2K plans;
3. Develop technical guidelines and standards;
4. Audit and certify agency compliance; and
5. Coordinate with the Office of Emergency Management, Prosecuting Attorney's Office and other stakeholders in the region on education and preparedness.

King County's Office of Emergency Management (OEM) is promoting Y2K preparedness to the public and county employees. To date OEM, in conjunction with the Executive Office and the Y2K Program Office, has prepared and distributed citizen and employee brochures on preparedness. Presentations for the public have been made in community forums and coordinated with community stakeholders. King County will continue to collaborate with private sector agencies in conducting "community forums" throughout King County.

The following summary represents the current status of King County's Y2K readiness efforts (as of July 31, 1999).

KING COUNTY Y2K SUMMARY

King County began its comprehensive Year 2000 (Y2K) program in 1996. The program consists of two major components. The first component is *remediation* to correct all year 2000 related problems. The second component is *emergency preparedness* to address unusual situations and significant events that might occur. This report reviews the County's overall effort to ensure essential services will continue uninterrupted as we transition into the year 2000.

The County has been proactive and is generally Y2K ready, with some outstanding issues to resolve (as detailed below). The County anticipates its systems will perform correctly and will provide uninterrupted support for its programs and public services. A Year 2000 Operations Plan has been developed to prepare for unusual situations during the Year 2000 transition period (December and January). Following is a summary of the County's Y2K readiness by business area.

REMEDIATION, of ALL COUNTY FUNCTIONS

Law, Safety, and Justice (LSJ) Business Function. Seven agencies provide public safety, law enforcement, detention, and criminal justice services for King County. Most systems that support essential services are Y2K ready. Work continues to change the fingerprint, mug shot and youth information systems, and these are expected to be Y2K ready by October. Status details of LSJ-related services follow.

1. **King County Sheriff's Office.** The King County Sheriff Office (KCSO) provides law enforcement, public safety, and investigative services to King County citizens. KCSO has conducted a comprehensive inventory of its essential hardware, software, applications, and embedded systems that support those vital services.

   - *Provide basic police services.* Police vehicles and fueling systems are Y2K ready. Mobile and portable 800-MHz radio communications are Y2K ready. The Computer-assisted dispatch (CAD) system, which supports police operations, is Y2K ready. Contingency plans are being developed for unusual events. Additional police officers will be on duty during year-end to handle unanticipated needs.

   - *Provide E-911 services.* KCSO is the Public Safety Answering Point (PSAP) for the unincorporated parts of King County and contract cities for police, fire, or medical emergencies. The PSAP is Y2K ready. Backup systems can reroute incoming calls to precincts or other PSAPs, if necessary.

   - *Provide criminal investigation.* The desktop applications and the mainframe application, *SEAKING,* which supports regional exchange of information, are Y2K ready. Washington State Patrol, other investigative agencies, and other providers have reported their systems are Y2K ready. Per State guidance, KCSO is retrofitting the ACCESS interface, and it is expected to be ready by Fall.

- *Provide fingerprint identification.* The *Automated Fingerprint Identification System (AFIS)*, which provides regional fingerprint processing for King County, City of Seattle, and other suburban cities, is being upgraded to Y2K readiness. Completion is expected in October. A contingency plan has been prepared.

- *Provide special operations.* Systems within the Special Operations Section (marine/dive unit, air support, traffic, search and rescue, bomb disposal, canine, SWAT) are Y2K ready.

- *Support civil processes.* Desktop systems that support issuance of court documents (subpoenas, court orders) and the enforcement of court ordered actions (seizures, evictions) are Y2K ready. Manual backup processes are in place.

- *Provide courthouse security.* Embedded systems that screen entry into County courthouses to enhance public safety are Y2K ready.

2. **King County Prosecuting Attorney's Office.** The Prosecuting Attorney's Office provides a variety of legal services to King County.

   - *Provide legal services.* Hardware, software, and embedded systems that support business functions for the prosecution of criminal, civil, and fraud cases are Y2K ready, except one *server,* one software product (*ABRA*), and one application (Brief Bank) to be upgraded Fall 1999. The *Prosecutors Management Information System (PROMIS)* mainframe application is Y2K ready.

3. **King County Superior Court.** The Superior Court conducts proceedings in a wide range of legal matters including Family Court Services, juvenile civil and criminal and adult civil and criminal cases.

   - *Provide court calendars.* Civil case management application is reported Y2K ready. Testing is underway for the Court Management Information System *(CMIS)* and the implementation will be completed in September.

   - *Process Court Cases.* Have received one vendor's letter of compliance and awaiting another vendor's letter for mission critical Video Court systems. Application for scheduling jurors is Y2K ready. Family Court Services *(FCS)* is being tested and implementation is planned for August. Other software and applications are reported Y2K ready. Contingency processes have been documented for mission critical department functions.

   - *Operate Courtrooms.* Systems that screen entry into County courthouses and courtroom duress alarms are Y2K ready.

4. **King County District Court.** King County District Court deals with legal matters not addressed in King County Superior Court. Legal proceedings take place in courtrooms maintained by support staff.

   - *Provide Court calendars.* An initial evaluation of hardware, software, applications, and embedded systems that support scheduling in the courts has been completed.

   - *Operation courtrooms.* Courtrooms generally operate independent of technology. No issues have been found with audiovisual equipment. Hardware, software, applications, and embedded systems that support the operation of courtrooms are being further evaluated.

5. **Department of Judicial Administration.** This department provides courtroom support, legal record keeping, trust and revenue management, and access to court records for the King County Superior Court, attorneys and the public.

   - *Provide Court calendars.* Washington State's calendar application, *SCOMIS,* has been verified as Y2K ready by Washington State Office of Administrator of Courts.

   - *Record legal documents.* Hardware, software, applications, and embedded systems that support the recording of legal documents are Y2K ready.

   - *Provide Court Orders.* Hardware, software, applications, and embedded systems that support providing court orders are Y2K ready.

   - *Provide access to legal documents.* Hardware, software, applications, and embedded systems that support the access to legal documents are Y2K ready.

6. **Department of Adult Detention.** This department provides safe, secure, humane, and cost-effective incarceration and inmate programs in partnership with other local, state, and federal criminal justice agencies.

   - *Maintain safe, secure environment for adult inmates.* Mission critical systems designed to ensure that inmates are housed safely and securely are reported Y2K ready. The software and application that provide required state and federal reporting are reported Y2K ready. Upgrade to the software that tracks inmate finances is expected in 3rd quarter. Equipment and power failure contingency plans have been prepared.

   - *Receive and release inmates.* Systems for receiving and releasing inmates, except the *Jail Electronic Mugshot System (JEMS),* are Y2K ready. Replacement plans are underway to upgrade JEMS; completion is expected in November. A contingency plan is being developed and will be presented to LSJ BAC in August.

7. **Department of Youth Services.** This department serves King County Superior Court and works with other government and social service agencies, communities, and families to develop and implement effective intervention strategies for juvenile offenders.

   - *Maintain safe, secure environment of juvenile offenders.* Thirty embedded systems have been identified as support systems for providing a safe and secure environment. Twenty-five of those systems are reported Y2K ready and five of those systems are still being assessed.

   - *Receive and release offenders.* The current application used to process all functions pertaining to juvenile offenders is being replaced. The implementation of the new application is scheduled for the end of October. A contingency plan has been prepared, but not yet reviewed by the LSJ BAC, in the event that the new application in not implemented on schedule.

General Government (GG) Business Function. Six offices or departments provide general services to King County agencies and the public. Most mission critical systems are Y2K ready. Validation for the E-911 and the 800 MHz radio systems, and replacement of the records and the elections systems are underway, and these are expected to be Y2K ready.

1. **King County Executive.** The King County Executive office is the executive branch of County government. The Executive is responsible for providing strategic direction for all governmental affairs, ensuring management of all County resources and funds, protecting the public trust, delivering services and approved activities, executing and enforcing all ordinances and State statutes within the County, and preparing and presenting plans for the present and future development of the County. The Executive maintains business offices where various support functions are performed.

   - *Provide data for preparation of County Budget.* Hardware and software within both the Office of Regional Policy and Planning and the Office of Budget have been tested and are Y2K ready. Mainframe applications have been remediated and are Y2K ready. Embedded systems have been evaluated and are Y2K ready.

   - *Provide Office of Human Resources Support.* Hardware and software within the Office of Human Resources Management (OHRM) have been tested and are Y2K ready. The *PARARISK* application relating to personnel is not Y2K ready and is in the process of being replaced. Embedded systems have been evaluated and are Y2K ready. Vendors, that provide the various benefit packages to the County, are being contacted to ensure that their services will not be interrupted.

2. **King County Council.** The King County Council is the legislative branch of County government. The thirteen-member elected Metropolitan County Council is the policy determining body of the County and exercises all legislative powers authorized under

the King County Charter. This includes adoption and enactment of ordinances, levy of taxes, appropriation of funds, establishment of compensation levels for County employees, and organization of administrative offices and executive departments. In addition to the Council chambers that includes various audio-video equipment, the Council maintains business offices where various support functions are performed.

- *Continue legislative duties.* Hardware and software have been tested and are Y2K ready. Applications have been remediated and are Y2K ready. Embedded systems have been evaluated and are Y2K ready.

- *Pass ordinances and motions.* Hardware and software have been tested and are Y2K ready. Applications have been remediated and are Y2K ready. Embedded systems have been evaluated and are Y2K ready.

- *Conduct public meetings.* The King County Courthouse audio video systems have been evaluated and certification as Y2K ready is pending.

3. **Department of Information & Administrative Services.** DIAS provides a wide-range of services supporting both the internal operations of the County and public services. Most essential systems are Y2K ready. Work is underway to complete Y2K readiness of two systems (recorders and E-911).

- *Maintain the County's Emergency Operations Center (EOC).* Systems that will allow independent operation of the County EOC are Y2K ready.

- *Provide 800 MHz radio service.* The regional *800-MHz* radio system infrastructure is Y2K ready.

- *Coordinate E-911 services between public agencies and private vendors.* The King County Public Safety Answering Point (PSAP) is Y2K ready. The regional E-911 communication system is Y2K ready, except for final verification statements from two network vendors. Twelve of eighteen PSAPs operated by local jurisdictions throughout the County have reported Y2K ready. Others are expected to report ready by September 1999.

- *Provide Data Center services.* The County's mainframe hardware and applications are Y2K ready. However, the latest mainframe operating systems software patches are being applied to enhance Y2K readiness. Expect completion October 1999.

- *Provide Wide-Area Network and Telecommunications services.* The County's data network systems and telecommunications systems, which support all agencies, are Y2K ready.

- *Issue licenses (animal, business, marriage, vehicle, and vessel).* Applications and databases that support licensing activity, including interfaces with Washington State agencies, are Y2K ready.

- *Administer elections.* The *Global Election Management System (GEMS)* ballot preparation and tabulation system is Y2K ready. The absentee signature verification system is Y2K ready. The voter registration system (mainframe-based) is Y2K ready.

- *Provide interoffice and US Mail service.* Applications supporting distribution of mail and other documents are Y2K ready.

- *Enforce animal regulations.* Systems supporting animal regulation and sheltering are Y2K ready.

4. **Department of Finance.** The Department of Finance provides fast, accurate, and professional financial services for the citizens and government of King County. It also processes financial transactions for the County and maintains the County's general ledger.

   - *Procurement services, payroll, accounts payable, and accounts receivable.* The Department of Finance processes financial transactions for the County. The enterprise mainframe applications, including *AIR* (accounts receivable), *BUC* (accounts payable), *POL* (payroll), and others that support these operations have been remediated and are Y2K ready. Hardware and software within the agency have been tested and are Y2K ready. Embedded systems have been evaluated and final certification for the payment processing system is being pursued.

5. **Department of Stadium Administration.** This department has provided a multipurpose entertainment facility. With the impending transfer of Kingdome assets, DSA is scheduled to be decommissioned and is not participating in the Y2K project.

6. **Department of Construction and Facilities Management.** This department provides King County government with facilities that return maximum value for the funds invested by taxpayers.

   - *Heat, cool, and light buildings.* Emergency power generators are not date-dependent and will operate past the Year 2000 date. HVAC upgrades are complete at KC Courthouse, Administration Building, KC Correctional Facility, Yesler Building and at 5 of 10 outlying buildings. HVAC upgrades are in process at the 5 remaining outlying buildings. Regional Justice Center (RJC) upgrades are being tested and completion is expected in October. Most building security systems are Y2K ready; validation of remaining systems is underway.

- *Run elevators.* Received letters of compliance from vendors for Elevator Control Systems in Courthouse complex, RJC, KCCF, KC Airport and KC North District Multi Service Center.

- *Repair building systems for other County departments.* Steps being taken now by DCFM will allow building systems to continue to operate as expected. Application software used to schedule building maintenance is Y2K ready. DCFM personnel will be available to handle repairs as usual.

Transportation and Land Use (TLU) Business Function. Five departments support all services related to building and land use permitting, community and regional parks, various recreational programs, solid waste disposal, surface water management, waste water control, roads, and transit operations. Below is a brief summary of each department.

1. **King County Department of Assessments.** This department is responsible for property evaluation, assessment of properties, and maintaining taxpayer records. The divisions are Commercial / Business Properties, and Residential. Key functions for this department include assessment of property values, and maintenance of property records.

    - *Assess property values and maintain records.* The enterprise mainframe applications that support the Department of Assessments, including assessments inquiry (ASE), property appraisal information (PAI), personal property valuation (PPV), levy file maintenance (ATB) and others, have been remediated and are Y2K ready. Hardware and software within the agency have been tested and are Y2K ready. Embedded systems have been evaluated and are Y2K ready.

2. **Department of Transportation.** This department is responsible for services related to transportation planning, community outreach on transportation issues, public transit, road construction and maintenance, and fleet management. The divisions include Administration, Transit, Transportation Planning, Road Services, and Fleet Administration. Key functions this department provides include maintenance of traffic signals, maintenance of county transportation routes, and providing transit service.

    - *Maintain traffic signals.* Traffic signal systems have been tested in the lab and in the field by Roads Services traffic engineering staff and are reported Y2K ready.

    - *Maintain County transportation routes.* Equipment associated with road maintenance is reported Y2K ready.

    - *Provide transit services.* Some hardware, software, applications and embedded systems that support transit services are still being assessed and remediated by division staff. Ninety-one percent of all systems are reported Y2K ready. One mission critical application is still being remediated. One of the three Prime computer systems has been remediated. The remediation completion date for the second system is scheduled for 8-13-99. Two mission critical embedded systems are still being assessed. The Y2K readiness of eleven mission critical suppliers has not yet been determined.

- *Provide fleet support services.* Hardware, software, applications, and embedded systems that support fleet services have been reviewed and are Y2K ready.

- *Provide transportation planning services.* Hardware and software are Y2K ready. The application review has begun and more documentation is needed.

3. **Department of Natural Resources.** This department is comprised of four divisions that provide service related to water quality, solid waste disposal, and environmental protection. The divisions include Water and Land Resources, Wastewater Treatment, Solid Waste and Solid Waste Marketing Commission. Key functions this department provides are collect wastewater, treat and discharge wastewater, receive solid waste from customers and transfer to landfill and disposal sites, operate storm water pump stations, and operate environmental control systems – pump stations and landfill gas system operations.

    - *Receive and transfer solid waste to landfill and disposal.* All of the systems to receive and transfer solid waste to the landfills for disposal are reportedY2K ready.

    - *Operate landfills.* All of the systems to operate the landfills are reported Y2K ready.

    - *Collect, treat, and discharge wastewater.* Systems have been tested and are reported Y2K ready. There will be staff on site during year-end to ensure that all systems are functioning properly. No Y2K related problems are expected.

    - *Provide flood warning.* The system is being examined and evaluated by the agency for Y2K readiness.

    - *Operate storm water pump station.* The system is being examined and evaluated by the agency for Y2K readiness.

4. **Department of Parks and Recreation.** This department is responsible for daily maintenance, minor improvements, beautification and stewardship of the park systems assets. The Recreation, Aquatics and Fair Division provides recreational, educational, and cultural opportunities and experiences for the public, including populations with special needs such as youth at risk and persons with disabilities.

    - Maintain park facilities & equipment. All park facilities and equipment have been tested and are Y2K ready. No interruption to services is expected.

5. **Department of Development & Environmental Services.** This department is responsible for Building Services, Land Use Services, and Administrative Services. Key functions for this department include issuing building permits, conducting building inspections and investigating fires. All systems have been tested and are Y2K ready.

   - *Investigate fires.* – The systems used to support fire investigation are Y2K ready and no interruption to services is expected.

   - *Conduct building inspections.* - The systems used to conduct building inspections are Y2K ready and no interruption to services is expected.

   - *Issue building permits.* – The systems used to issue building permits are Y2K ready and no interruption to services is expected.

Health and Human Services (HHS) Business Function. Two departments support health and human services for King County. One mission is to enhance the quality of life, protect rights, and promote the self-sufficiency of our region's diverse individuals, families, and communities. A second mission is to achieve and sustain healthy people and communities throughout King County by providing public health services that promote health and prevent disease.

1. **Department of Public Health.** The department provides support for emergency medical services, preventative health, environmental health, community-oriented primary care, substance abuse, regional clinics and health centers, and health administration. Hardware, software, applications, and embedded systems have been assessed, and most systems are reported Y2K ready. Review continues for a few components, and determination of their status is expected to be complete in September.

   - *Provide emergency medical aid at incidents.* Ambulances and medical emergency equipment are Y2K ready.

   - *Provide health care at clinics.* Administrative applications and databases on office desktop computers at the clinics are Y2K ready. The *Public Health Information System* (PHIS) is Y2K ready.

   - *Maintain link with area hospitals in treatment and distribution of patients.* Administrative applications and databases that interface with hospitals are Y2K ready, except for the *Practice Partner Scheduler* interface with Swedish Hospital, which will be upgraded by October 1999.

   - *Provide medical examiner services.* Administrative applications and databases that support medical examiner services are Y2K ready.

- *Provide environmental health services.* Administrative applications and databases that support environmental health services are Y2K ready, except the *Decade* health permit application will be replaced by October 1999.

2. **Department of Community & Human Services.**

- *Assign public defenders.* Hardware, software and applications in the Office of Public Defense are reported Y2K ready. Hardware at *The Defender Association* was tested by the Y2K technical support staff. Test findings were reported to the department. More work may be needed to assess the readiness of the three other defender agencies that provide legal support services.

- *Provide mental health data services.* Hardware and software are reported Y2K ready. Three non-compliant applications are being corrected.

EMERGENCY PREPAREDNESS, King County Y2K Operations Plan.

King County must be ready for unanticipated situations during the last few days of 1999 and the beginning of the year 2000. It is important that King County government makes a smooth transition into the year 2000 and set an example for other government agencies as well as private businesses. For a complete copy of the Y2K Operations Plan as written by Office of Emergency Management, refer to *www.metrokc.gov/prepare*.

King County will observe the following policies and procedures:

- The King County Emergency Operations Center (EOC) will open no later than 0500 on December 31, 1999 in order to monitor the transition to the year 2000 around the world. It will remain open as long as required to check systems and coordinate emergency events.

- County department directors will ensure that managers have addressed potential Y2K system failures to mission critical functions and have taken appropriate steps to correct identified problems.

- Department directors will ensure that schedules and procedures are in place and implemented for the verification and testing of systems that supply essential county services prior to the beginning of the new year.

- Department directors will ensure that contingency plans are in place for all mission critical functions should technology based systems fail.

- Department directors and managers will ensure that appropriate staff is in place to initially check mission critical systems as the New Year begins. More thorough systems checks will be conducted prior to the start of the first business day of 2000. This may include limiting or canceling vacation requests of mission critical personnel, and/or scheduling staff to work overtime.

RESPONSIBILITIES

The following are basic responsibilities for emergency management operations as they relate to Y2K issues. These responsibilities are in addition to those identified in the King County Emergency Management Plan. Department level operating procedures detail how individual Departments shall perform their responsibilities. It is expected that all political subdivisions, businesses, volunteer organizations and private citizens will take steps to mitigate potential problems and plan for the unexpected.

All County Departments and Agencies shall:

- Work with members of the Year 2000 Program Team to update hardware, software, applications and embedded systems, and develop contingency plans to address Y2K issues of mission critical systems.

- Have contingency plans in place for failures of systems that are not owned by the county but are critical to the county's ability to provide mission critical services.

- Support Emergency Management activities regarding Y2K including public education campaigns, employee education, and EOC activation needs.

- Assign a representative to provide information to the EOC reference the status of their department. That representative will contact the EOC by telephone, 800 MHz radio, or personally, to report the status of their department. Reporting times may vary depending on the complexity and expanse of systems, but all departments are expected to check in no later than 1600 on January 1, 2000. First response agencies, those who are charged with direct care to specific populations, and those with direct responsibility to infrastructure systems will provide representatives to the EOC.

- Assign personnel to work in the King County Joint Information Center to coordinate public information from county departments and to ensure that King County government is sending a united message. The Executive's Communication Director will lead the Joint Information Center.

ACCOMPLISHMENTS

Y2K Public and Employee Preparedness Educational Outreach

King County's Office of Emergency Management (OEM) is promoting Y2K preparedness to the public and county employees. To date OEM, in conjunction with the Executive Office and the Y2K Program Office, has prepared and distributed citizen and employee brochures on preparedness. Presentations for the public have been made in community forums and coordinated with community stakeholders. King County will continue to collaborate with private sector agencies in conducting "community forums" throughout King County.

Business Continuity Planning

The Office of Emergency Management is encouraging Departments to review their current disaster plans to ensure that Y2K issues are addressed, their plans and procedures are current, and employees are trained. A contingency planning workshop was hosted in mid-July to assist representatives from various county departments to improve their internal plans. Our office will continue to support agencies with emergency planning as we move toward the year 2000.

For more information on King County Y2K issues, please see the website at www.metrokc.gov. If there are any questions relating to this report, please call Marilyn Pritchard, Y2K Communications Specialist, at (206) 205-1495.

Mr. HORN. Thank you very mucn. Mr. Marty Chakoian is the year 2000 project manager for the city of Seattle. Thank you for coming.

Mr. CHAKOIAN. Thank you. And on behalf of Mayor Paul Schell, I'd like to welcome you to Seattle.

The city of Seattle, of course, provides essential life and safety services—police, fire protection, emergency medical services, traffic control—to our half-million residents. We also are directly responsible for many local utilities: electricity, drinking water, sewer and drainage services, solid waste removal. Those are services provided by city departments, and you'll be hearing from them on the next panel.

Many of these services depend to one degree or another on computer systems, and they will not be disrupted by the year 2000 problem.

I was asked last February to establish a central project office to coordinate this effort, city-wide. Since then, we've adopted a date standard, promulgated a formal methodology. We've trained departments on how to use tools and techniques to be successful. We've prioritized the work of the city. We have an overall project plan with activities and milestones.

And we're assisting departments directly with their embedded systems, the evaluation of products and services, testing, and contingency planning. We're not finished yet, but we will finish, and we'll finish on time, and we've laid the foundation to ensure success.

Let me tell you where we are at this point. Over 93 percent of our physical computer systems are now Y2K compliant. The city's fiber backbone data network has been upgraded and is compliant. A new police 911 center has been installed, and we're doing an end-to-end test with U.S. West this week.

Likewise, we've evaluated our radios, mobile data terminals, other essential equipment, and determined it to be Y2K compliant.

Of our 90 mission-critical applications, over 80 percent of those have now been remediated. And that includes the most critical things, like police and fire dispatch, electrical energy management system, water laboratory information system, our library system, our municipal court system, our core financial and payroll systems.

The ones that we're still working on, things like a system in our parks department that schedules ball fields, a receipt payment system for building permits, and the system that assigns staff to events at the Seattle Center, those systems, as well as our minor systems, will also be remediated.

But we're not stopping there. We have, in addition, a formalized testing program that we require our applications to go through under the direction of the project office, using a test plan template that we've adopted from the State. We've also gone through our embedded systems to ensure that our water and electrical systems, our wastewater system, solid waste systems, communications equipment, fire boats, police stations, emergency medical equipment, even the equipment at our zoo and our aquarium is Y2K compliant.

We're working with our vendors, with other government agencies to ensure that they likewise will be able to continue to work with us. And each city department is developing contingency plans. Some of those have already been exercised. We're going to have a city-wide exercise in October.

And, like other government agencies, we're working closely with the public. We have materials now at our libraries and community centers. We've produced a video that we're sharing with the public on how neighborhoods can work together. And we're doing more and more direct personal contact with our senior citizens and community groups.

One thing, however, does concern us about the year 2000. Seattle, as you know, is an international city. We're going to be hosting the World Trade Organization this November. Port of Seattle is the fifth largest port in dollar volume in the Nation, and the Port of Tacoma not too far behind. It's been estimated that, per capita, Washington State is the most trade-dependent State in the country, with one of every four jobs related to international trade.

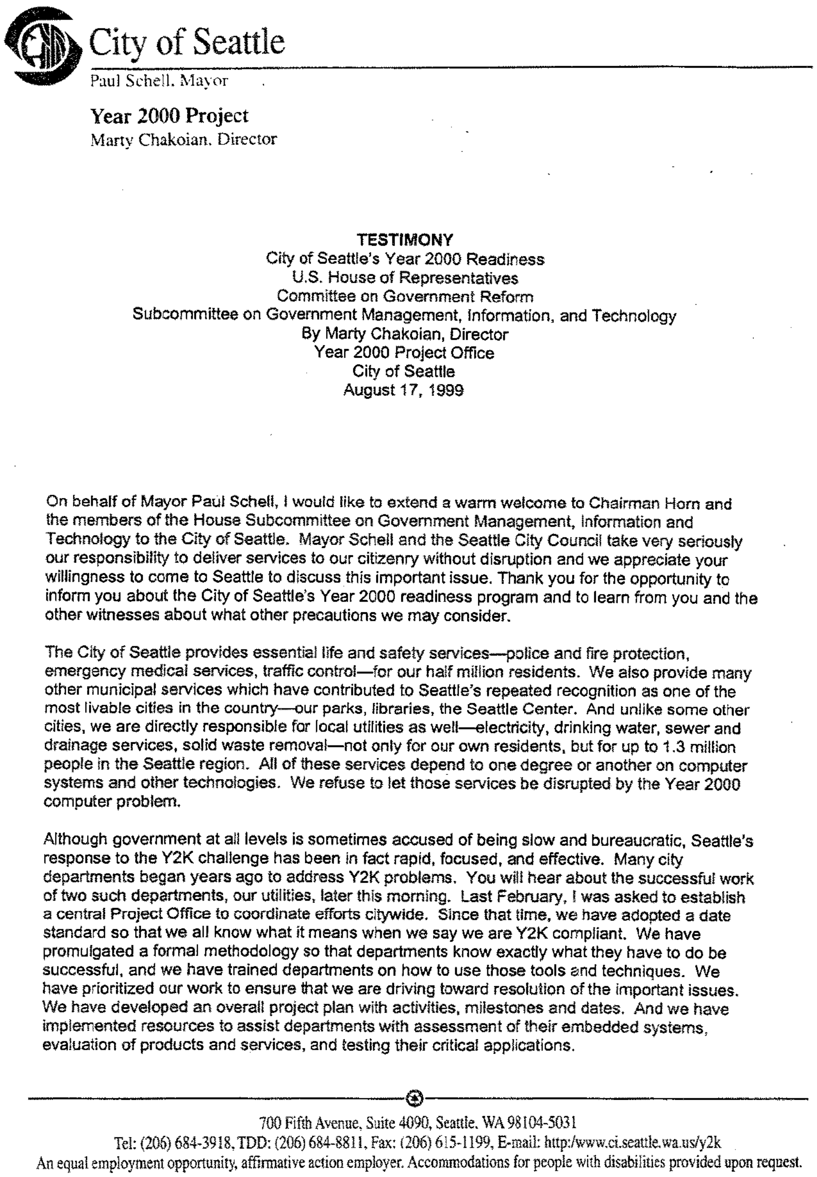
And so I was concerned when I read the testimony of Jacquelyn Williams-Bridgers, who is the Inspector General for the Department of State, talking to the U.S. Senate, reporting that the global picture is cause for concern.

She says that the global community is likely to experience Y2K-related failures in every sector, every region, and at every economic level. She says that this may result in creating economic havoc and social unrest in some countries, and in addition to the impact on the families living in those countries, she says that it could extend to the international trade arena, where a breakdown in any part of the supply chain would have a serious impact on the United States and world economies.

So we in Seattle are very grateful for the work that your committee has done to ensure that the Federal Government will be Y2K compliant, and we would appreciate your continued support of those efforts, as well as working with the Federal agencies. We're trying to ensure that our international trading partners can also be Y2K compliant and continue to work with us in the future.

In conclusion, I'd like to simply invite you to come back to Seattle to spend New Year's Eve with us at the Seattle Center if you happen to be in the neighborhood. We're going to have over 100,000 people there, and I think it's going to be a great place to ring in the new year. Thank you.

[The prepared statement of Mr. Chakoian follows:]



City of Seattle
Paul Schell, Mayor

Year 2000 Project
Marty Chakoian, Director

TESTIMONY
City of Seattle's Year 2000 Readiness
U.S. House of Representatives
Committee on Government Reform
Subcommittee on Government Management, Information, and Technology
By Marty Chakoian, Director
Year 2000 Project Office
City of Seattle
August 17, 1999

On behalf of Mayor Paul Schell, I would like to extend a warm welcome to Chairman Horn and the members of the House Subcommittee on Government Management, Information and Technology to the City of Seattle. Mayor Schell and the Seattle City Council take very seriously our responsibility to deliver services to our citizenry without disruption and we appreciate your willingness to come to Seattle to discuss this important issue. Thank you for the opportunity to inform you about the City of Seattle's Year 2000 readiness program and to learn from you and the other witnesses about what other precautions we may consider.

The City of Seattle provides essential life and safety services—police and fire protection, emergency medical services, traffic control—for our half million residents. We also provide many other municipal services which have contributed to Seattle's repeated recognition as one of the most livable cities in the country—our parks, libraries, the Seattle Center. And unlike some other cities, we are directly responsible for local utilities as well—electricity, drinking water, sewer and drainage services, solid waste removal—not only for our own residents, but for up to 1.3 million people in the Seattle region. All of these services depend to one degree or another on computer systems and other technologies. We refuse to let those services be disrupted by the Year 2000 computer problem.

Although government at all levels is sometimes accused of being slow and bureaucratic, Seattle's response to the Y2K challenge has been in fact rapid, focused, and effective. Many city departments began years ago to address Y2K problems. You will hear about the successful work of two such departments, our utilities, later this morning. Last February, I was asked to establish a central Project Office to coordinate efforts citywide. Since that time, we have adopted a date standard so that we all know what it means when we say we are Y2K compliant. We have promulgated a formal methodology so that departments know exactly what they have to do be successful, and we have trained departments on how to use those tools and techniques. We have prioritized our work to ensure that we are driving toward resolution of the important issues. We have developed an overall project plan with activities, milestones and dates. And we have implemented resources to assist departments with assessment of their embedded systems, evaluation of products and services, and testing their critical applications.

City of Seattle departments, working with the staff of the Project Office, have made significant progress in defining, prioritizing, and fixing their Y2K problems. We are not finished yet. But we will finish, and we will finish on time. A regular review by an independent consulting firm verifies that the City is doing the right things the right way and at a pace that will bring us success. Each bimonthly follow-up with departments shows continuing progress. While much work remains, the standards and coordination implemented since February have laid the foundation for the City's ability to ensure continuity of service in January of 2000 and beyond.

Let me present briefly the results we have achieved:

Computing and Communications Infrastructure

One important aspect of the Y2K project has been to ensure that the City's desktop computers and local area networks are fully Y2K ready. We have inventoried 8120 PCs used by City departments; of those, 7536, or 92.8%, are compliant. The remainder are being upgraded or replaced. The deadline for completing this work is August 31. The City's fiber backbone data network is being upgraded and a new Police 911 Center is being installed at the new West Precinct; although this system is certified by the vendor as Y2K compliant, a full scale test is scheduled in conjunction with US West for later this month. Likewise, other key elements of our computing and communications infrastructure, including radios and mobile data terminals, have been determined to be Y2K compliant.

Computer Systems and Applications

Most department efforts have been focused on fixing applications which support the City's primary business functions. Departments have identified 90 mission critical applications. As of this report, 72 of these either have no date-related problems, or have been fixed or replaced. The remaining 18 systems are in various stages of replacement with new software. Systems which are finished include police and fire dispatch, our electric utility's energy management system, our water utility's laboratory information system, our library system, our municipal court case scheduling system, and our core financial and payroll systems. In other words, our highest priority systems are finished. Systems which are still being worked on include those which schedule ballfields for our Parks Department, receipt payments for building permits, and assign staff to events at the Seattle Center.

In addition to completing this work, departments are upgrading or replacing their minor applications: those small systems that provide useful information or automate simple tasks. In most cases, such upgrades can be done in a day or less.

Testing

When departments have finished fixing their mission critical applications, our approach is to certify each system as compliant through additional rigorous, formal testing under the review of the Y2K Project test team. We have established a testing methodology, a test plan template, test labs, and separate testing regions for our mainframe and UNIX systems. The purpose of this final quality assurance effort is to ensure that nothing has been missed in fixing or upgrading our core systems.

Embedded Systems

The term embedded systems is used to refer to computer chips and software embedded in equipment that is used in day to day business operations. Examples include HVAC systems, fuel pumps, alarms, and process controllers.

The City has now completed an aggressive examination of its embedded systems, using both expert City staff and consultants. The utilities have reviewed controllers used in the monitoring and distribution of water and electricity and in the removal of wastewater and operation of the solid waste transfer stations. The Police communication equipment and Fire stations, fire boats, and emergency medical equipment have been carefully inventoried and assessed. Even the systems which help to operate the Zoo and the Aquarium have been surveyed and addressed to ensure that animal life will not be jeopardized by Y2K related errors.

Vendors and Suppliers

Like most public or private organizations, the City of Seattle cannot function without the products and services it receives from its business partners. We depend not only on cooperation and support from other government agencies—the federal government, the State of Washington, King County—but also from the private sector. We have therefore identified and begun surveying our most critical suppliers: large firms such as our telecommunications provider, our banks, and others, along with smaller companies on whom we depend for supplies and equipment. Thus far we are reassured by the serious approach which these companies are taking to address their own Y2K issues; any lapses in their ability to serve us will be addressed in our contingency plans.

Contingency Planning

The one certainty about Y2K is that something somewhere will go wrong. Therefore, departments are developing contingency plans to help ensure that the public will continue to receive basic services without interruption. Department staff are looking at areas of potential vulnerability and identifying realistic short term work-arounds should any of our own systems fail or our vendors or suppliers be unable to meet their obligations to us. Some departments have already conducted table-top exercises to test and refine their contingency plans. A city-wide exercise is scheduled for October.

Public Involvement

Seattle city government's focus during the first half of 1999 was to get its own house in order: to inventory, assess, and fix its own Y2K problems. However, Seattle's success in moving smoothly into the new year will be measured not just in how government services perform, but in how our whole community transitions. Individual and neighborhood preparations are as important as the preparations of city departments. While some excellent work has been accomplished by the city's Emergency Operations Center in promoting general preparedness through large scale community events and ongoing programs, a more comprehensive, Y2K specific preparedness program is now under way. This effort consists of a combination of written materials provided to our libraries, community centers, and neighborhood offices, a video on neighborhood preparedness produced by our Seattle Disaster Aid and Response Team (a copy of which has been provided to the Committee), and by direct personal outreach to community groups, business councils, and senior citizens. Only by providing our communities with complete and thorough information and the resources to act on that information can we work in partnership to ensure that we are ready for whatever faces us.

Collateral Benefits

Y2K efforts in the City and elsewhere are generally focused on assessing risk and fixing specific problems; our explicit goal is that the City will be able to operate next year just as it does today. Thus, a significant investment of effort is being made merely to maintain the status quo.

Nonetheless, many aspects of the City's Y2K program will have a lasting, positive impact and are therefore worth noting. These include

- A better understanding of key business processes and dependencies
- Increased quality, quantity, and accessibility of documentation of business systems
- Identification and retirement of obsolete applications

- Improved application inventories and license management
- Renewed attention to project management disciplines and techniques
- Recognition of the need for change management
- Formalization of the testing process and creation of test environments
- Establishment and implementation of City standards for desktops and networks
- Increased functionality of new applications implemented to solve Y2K problems
- Upgrading of the City's computing and communication infrastructure
- Development of contingency plans for business continuity

If continued and built upon, these advances can create the foundation for a significantly higher level of professionalism and performance across the City's computing environment in the Year 2000 and for years to come.

Concerns

If, as I have said, the City of Seattle is taking deliberate, direct action to ensure that our systems and our citizens will be ready for Year 2000, and if those actions are producing the results we need, then what are our concerns for the turn of the century?

I believe that New Year's morning will find Seattle in good shape. Our lights will work, high quality water will flow, the toilets will flush, the traffic signals will function perfectly normally. Our police and fire departments may be exhausted from an unusually busy night, but the 911 system, the dispatch systems, the information systems they rely on will be operating reliably. When we open for business on the morning of Monday, January 3, I believe that the public will find that our services are available and that few if any manual work-arounds have been implemented.

Seattle, however, does not live and work in isolation. I am concerned that over the course of the first and second quarters of the year 2000, disruptions in world economies and international supply chains could have a serious effect on us.

While we may appear to some to be isolated and provincial, Seattle is in fact an international city. We will be hosting the World Trade Organization's Ministerial meeting in November and December of this year. In dollar volumes, the Port of Seattle is the fifth largest port in the nation. In 1997, over $23 billion dollars in imports and another $10 billion in exports flowed through our port facilities. The Port of Tacoma, just a few miles to the south, is not far behind, with over $20 billion in imports and exports annually. We rely on our international trading partners to buy our goods and our products, and to provide us the raw materials and manufactured items we need. Patricia Davis, President of the Washington Council on International Trade, testified before the U.S. International Trade Commission in May of last year that, per capita, Washington state is the most trade dependent state in the country, with one of every four jobs related to international trade. This includes not only such giants as Boeing, Microsoft, and Weyerhaeuser, but smaller retail and wholesale companies, manufacturing firms, and farms throughout the state.

I therefore read with a great deal of concern the testimony of Jacquelyn L. Williams-Bridgers, Inspector General of the Department of State, before the United States Senate's Special Committee on the Year 2000 Technology Problem. In reviewing the efforts of other nations to address their Y2K challenges, Ms. Williams-Bridgers concluded that "the global picture that is slowly emerging is cause for concern." The results of the State Department's extensive research abroad found that "the global community is likely to experience varying degrees of Y2K-related failures in every sector, every region, and at every economic level." In some countries, this includes "a clear risk that electricity, telecommunications, and other key systems will fail, perhaps creating economic havoc and social unrest." The result would not only impact families living in those countries, but, to quote Ms. Williams-Bridgers, "will likely extend to the international trade arena, where a breakdown in any part of the supply chain would have a serious impact on the U.S. and world economies."

If not for reasons of compassion and humanitarianism, then at least in support of economic self-interest, I would urge the State Department to accelerate its efforts in assisting foreign nations with Y2K remediation and, at this late date, with serious contingency planning to minimize the impacts of the disruptions which will inevitably occur. I am pleased that the Department of State acknowledges its responsibility to take the lead in this area; I am discouraged to learn that little has yet been done to address potential supply chain disruptions originating in other countries. To the extent that resources can be organized now to assist the most severely impacted regions and economic sectors, both before and after the date rollover, the Puget Sound region and the nation will be well served.

On behalf of the City of Seattle, I want to thank you for bringing your committee here. Your willingness to come and to listen and to engage in a dialog about our Year 2000 successes and concerns demonstrates a respect and interest that is greatly appreciated. I am grateful for the opportunity to present this information to you, and to learn from the information that others have presented. And, if you're in the neighborhood, I invite you to spend New Year's Eve with a hundred thousand Seattle area residents at the Seattle Center. I think you will find Seattle a very good place to ring in the New Year.

Mr. HORN. Well, I appreciate the offer. Ms. Dunn says be sure the elevator works. And we'll get into microdots and microchips later.

But I have already committed myself, in almost every hearing, to do my usual trip to California from Dulles International to Los Angeles International. And I've got the FAA Administrator, who is a very able person, to also go on a trip. I've offered the east-west stuff, but last time she was going from National in Washington to La Guardia in New York. And I told her, "Hey, just don't upset the controllers before I get on board, if you don't mind." So I might take you up on that.

OK. Last member of this panel is Barbara Graff, the emergency preparedness manager for the city of Bellevue. Thank you for coming.

Ms. GRAFF. Thank you. Good morning, Congressmen Horn and McDermott. Congresswoman Dunn, welcome home. In decades past, Bellevue has been referred to as the bedroom community of Seattle. These days, we refer to Seattle as the dining-room community of Bellevue.

I am the emergency preparedness manager for the city of Bellevue, and though my costume implies that I am a single department representative, our division is in charge of an all-hazard program for all city services and departments.

Our city has been dealing with the problems posed by the year 2000 using a team effort. The technological problems associated with Y2K have been mitigated under the leadership of our Information Services Department. An interdepartmental preparedness plan to deal with any consequences has been developed by our emergency preparedness organization.

My division has been responsible for educating the public. And our city council and senior staff team have been responsible for providing support, leadership and resources to prepare the community.

The city of Bellevue has been actively addressing year 2000 issues for several years. A strategic plan was developed in 1997. 24 major computer systems were evaluated to determine the cost benefit of replacement versus modification. Programming updates have been completed, tested and implemented for all systems for which modification was determined appropriate. The remaining seven systems are in various stages of replacement, and will be completed and operational by the end of September.

As a precautionary measure, however, contingency plans have also been developed for remediating or running parallel modified systems through the new year.

Research has been conducted on the more than 500 products which contain process controllers or microchips, and an independent consultant has recently studied, tested and validated the city's Y2K remediation work.

Early this year, the city's Emergency Operations Board developed a Y2K readiness plan outlining contingency measures to ensure no disruption of critical services for our customers, similar to the State of Washington's goal. This augments a comprehensive all-hazard emergency operations plan that had already been in place for 8 years. This includes: one, an aggressive public outreach self-preparedness campaign; two, working closely with our partners in service delivery, such as Puget Sound Energy, Overlake Hospital, and the Seattle Public Works Department; and three, preparing our own employees so they'll be ready to assist the community in any circumstance.

Our Emergency Preparedness Division has applied the same philosophy to Y2K preparedness that we have given to the 50,000 people in our community over the last 8 years about earthquake preparedness. The better informed our community is about potential problems, the more likely that they will take appropriate self-preparedness steps and the less likely that emergency services will be overwhelmed.

We're making use of all possible public education formats, including videos on local governmental and community college channels, newsletter and newspaper articles, classes and workshops. Our "Stomp on the Millennium Bug" brochure is available at all city facilities, it's on our city webpage, and we display it throughout the community. We also make sure it's in the hand of every fifth grader at all public and private schools. They're the ones who get their parents to take action.

We've met with the Chamber of Commerce and Bellevue Downtown Association regarding specific concerns for small to medium-sized businesses who may not have the resources or inclination to engage in general disaster preparedness, let alone prepare for this specific threat.

We've directly mailed a letter to all city B & O taxpayers and the chamber of commerce mailing list providing resources and information to prepare their businesses.

We're encouraging neighborhoods to organize themselves according to the Strengthening Preparedness Among Neighbors program that recognizes that many times your best source of help in region-wide disasters is your neighbor.

Emergency generator power is available at parks department community centers, which could be used as mass care shelters. Protocols are already in place to fuel our vehicles, top off our water tanks, utilize manual procedures where appropriate, and assign appropriate staff to work through critical time periods.

Our emergency management organization has already conducted two tabletop exercises this year to identify any weakness in our contingency plans and improve our operational readiness.

Bellevue, like many jurisdictions, will be activating our Emergency Operations Center on December 31st, and we will be appropriately staffed and ready to respond to any circumstance. Arrangements are already in place with other important partners, such as our ham radio operator group, churches, the Red Cross, service clubs, and city volunteers.

A great deal of progress has been made. Many people are preparing themselves for the same harsh conditions that a winter storm would bring: cold weather, scattered power outages, difficulties with communications and transportation. A lot of work has been done to fix the technological problems. Still, we believe there is reason for concern.

Triaged, or sorted, fixes for many organizations means that a lot of work remains undone, opportunists with malicious intent, just-in-time delivery of goods and services, and the ripple effect of inadequate fixes for basic problems.

Although no organization, public or private, can realistically offer a guarantee that Y2K will have no effect on their service, we can offer the assurance that we're ready to meet any consequence of the date change.

Bellevue is treating Y2K as an opportunity to practice consequence management. First, we're aggressively mitigating our own technological problems before they can occur. Second, we're strengthening the partnership we had already created with our community in disaster preparation. Third, we're preparing to deal with whatever consequence may come our way in the new year. In any event, at the end of this year, we'll be better prepared to have our community and governmental services ready for the next earthquake or real disaster.

Bellevue, however, is only one part of the picture. There are countless agencies related to each other through the common use of products and services. The year 2000 will be, among other things, a great revelation of just how dependent we are on one another. It's also an extraordinary opportunity to strengthen our ability to count on one another. Thank you very much.

[The prepared statement of Ms. Graff follows:]

Y2K Congressional Field Hearing, Tuesday, 8/17, Seattle, WA

Good morning. My name is Barb Graff. I am the Emergency Preparedness Manager for the City of Bellevue, Washington. Our City has dealt with the problems posed by the Year 2000 using a team effort. The technological problems associated with Y2K are being mitigated under the leadership of our Information Services Department. An interdepartmental preparedness plan to deal with any consequence has been developed by our emergency preparedness organization. My division has been responsible for educating the public. And our City Council and senior management team have provided support, leadership, and resources to prepare our community.

The Plan

The City of Bellevue has been actively addressing Year 2000 issues for several years. A strategic plan was developed in 1997. Twenty-four major computer systems were evaluated to determine the cost benefit of replacement versus modification. Programming updates have been completed, tested, and implemented for the systems determined appropriate for modification.

The strategic plan also identified several systems, including public safety, maintenance and operations, and utility customer service as needing replacement. These systems are in various stages of replacement and will be completed and operational by the end of September. As a precautionary measure, contingency plans have also been developed for remediating or running parallel modified systems through the new year.

Research has been conducted on the more than 530 products which contain process controllers (microchips) including telephones, card keys, elevators, alarms, telemetry, irrigation, etc. An independent consultant recently studied, tested, and validated the City's Y2K remediation work.

Early this year, the City's Emergency Operations Board developed a Y2K Readiness Plan outlining contingency measures to ensure no disruption of critical services to our customers. Three vital ingredients to this planning effort include: 1) an aggressive public outreach campaign to encourage our community to take appropriate preparedness actions; 2) working closely with our partners in service delivery such as Puget Sound Energy, Overlake Hospital, Seattle Public Utilities, SeaFirst Bank of America, King County Health Department, and U.S. West Communications, among others; and 3) preparing our employees so that they will be ready to assist the community in any circumstance.

The progress

The Emergency Preparedness Division has applied the same philosophy to Y2K preparedness as it has used to teach 50,000 people over the last 7 years about earthquake preparedness. The better informed our community is about Year 2000 potential consequences, the more likely they will take appropriate self-preparedness steps and the less likely emergency services will be overwhelmed by demands for service.

We are making use of all possible public education formats including videos on local governmental and community college channels, newletter and newspaper articles, classes and workshops. Our Stomp on the Millennium Bug brochure is available at all City facilities, on our City web page, on display throughout the community and has been distributed to students in our public and private schools.

We have met with the Chamber of Commerce, Bellevue Downtown Association and Downtown High-Rise Association regarding specific concerns for small to medium sized businesses who may not have the resources or inclination to engage in general disaster preparedness and have not prepared for this specific threat. A letter was mailed in early March to all City B&O tax payers and the Chamber of Commerce mailing list providing resources and information to prepare their businesses. We are encouraging neighborhoods to organize themselves according to the Strengthening Preparedness Among Neighbors program recognizing that many times your best source of help in region-wide disasters is your neighbor.

The City has spent over $2 million to get Y2K ready and we feel confident that the City will be prepared. We are completing the remediation or replacement of all central applications, network and telephone systems, desktop PCs, and are now working on embedded chips and continue to verify the readiness of all vendors and service providers.

The Fire Prevention Division has been working with property managers and building owners regarding fire safety systems and alarms. City facility management staff are working with vendors of embedded chips in testing systems in our buildings. Emergency generator power is available at Parks Department Community Centers which could be used as mass care shelters. Protocols are in place to fuel vehicles, top off water tanks, and assign appropriate staff to work through critical time periods.

The Emergency Operations Board and Emergency Management Committee have conducted two tabletop exercises this year to identify any weaknesses in our contingency plans and improve our operational readiness.

Bellevue, like neighboring cities, King County, and the State, will be activating our Emergency Operations Center the evening of 12/31/99. We will be appropriately staffed and ready to respond to any circumstance. Arrangements are in place with other important partners such as the Eastside Amateur Radio Support group, churches, Red Cross, service clubs and city volunteers.

The prognosis

A great deal of progress has been made. Many people are preparing themselves for the same harsh conditions a severe winter storm would produce – cold weather, scattered power outages, difficulties with communication and transportation. A lot of work has been done to fix the technological problems. There remains, however, reasons for concern.

Triaged fixes for many organizations means that a lot of work remains undone, opportunists with malicious intent, just-in-time delivery of goods and services, and the ripple effect of inadequate efforts to fix the basic problems.

Although no organization, either public or private, can realistically offer a guarantee that Y2K will have no effect whatsoever on their product delivery or service, we can offer the assurance that we are "ready" to meet any consequence of the date change.

The City of Bellevue is treating Year 2000 as an opportunity to practice consequence management. First, we are aggressively mitigating our own technological problems before they can occur. Second, we are strengthening the partnership we had already created with our community in preparation for disasters. Third, we are preparing to deal with whatever consequences may come our way in the new year. In any event, we will have better prepared our community and governmental services for the next earthquake or other disaster.

Bellevue is only one part of the picture. There are countless agencies related to each other through the common use of products and services. The Year 2000 will be, among other things, a great revelation of just how dependent we are on each other. It will also be an extraordinary opportunity to strengthen our ability to count on one another.

Thank you for your time and attention.

- Cold & Flu medications
- Eye Wash
- Antiseptic or hydrogen peroxide
- Basic first aid kit

❑ Sanitation
- Toilet Paper
- Feminine supplies
- Plastic garbage bags & ties
- Plastic bucket with tight lid
- Household chlorine bleach
- Soap, liquid detergent and waterless anti-bacterial soap
- Antibacterial wipes

❑ Tools and Supplies
- Mess kits or paper plates and plasticware
- AM/FM radio and flashlights with extra batteries
- Fire Extinguisher, small canister, ABC type
- A *safe* alternate heat source or warm blankets and sleeping bags

❑ Prescription Medications
- Have at least 3–7 days of prescription medications on hand before the New Year

❑ Activities for children who have no TV or video games
- Puzzles, games, books, coloring books and crayons

❑ Fill up the fuel tanks of all your vehicles

❑ A small amount of cash in small bills (in case cash machines and credit card service is interrupted)

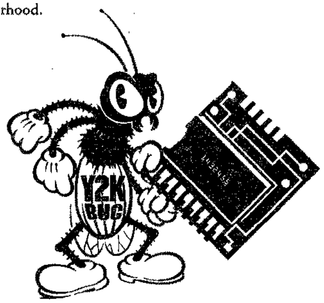
m4182-1/99.pm6.5

If there are interruptions in basic services such as water, power and communications:

❑ Listen to your battery operated AM/FM radio for information from your emergency service providers. Be sure you have extra batteries so that you can use the radio for up to a week.

❑ Only call 911 to report a life threatening emergency. Otherwise, stay off the telephones and cell phones.

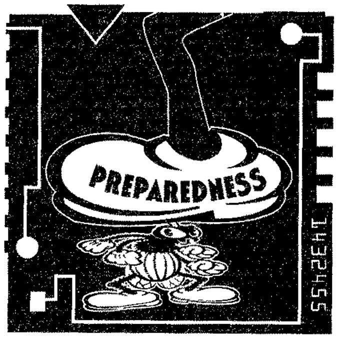
❑ Organize your neighborhood before the new millennium to help each other respond to any interruptions created by the change in new year. The City of Bellevue has a program called Strengthening Preparedness Among Neighbors that is designed to help neighborhoods prepare for disasters. Call 425-452-7923 for more information or to schedule a program for your neighborhood.



GET PREPARED NOW

Visit our internet site www.ci.bellevue.wa.us

STOMP ON THE MILLENNIUM BUG



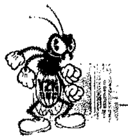
YEAR 2000 AND YOU

Introduction:

In the early days of computers, programmers created a two digit year field for the date as a way to conserve the amount of memory space in the computer. Therefore, 1998 is read as 98. When the Year **2000** comes, some computer systems will think it is **1900**. This may not affect some systems that do not use date and time functions in their system. However, this problem may dramatically impact any system that calculates, or schedules, whether it be calculating your age for retirement benefits, or reporting scheduled maintenance for equipment and vehicles.

Since 1996, the City of Bellevue has been working to minimize the impacts of the Millennium Bug on City services. This includes assessing all equipment and systems to see if embedded chips are used, replacing and/or updating computers and systems to be "Y2K compliant" and creating contingency plans to respond should there be service interruptions from agencies that provide electricity, water, sewer treatment and other supplies.

Preparing our community for a disaster, whether it be natural or technological, must be a partnership between government and citizens. We are doing our part to be prepared for any consequences the Year 2000 may bring. Here are some ways that you, as a citizen, can join the partnership and prepare your home and your family.



Safeguarding your records

❑ Get paper records of your finances (from your bank, mortgage company, investments and retirement fund, etc.)

❑ Watch for improper billing and be sure you are not being overcharged.

❑ Get a copy of your credit report.

Preparing Your Home

❑ Contact the maker of your home thermostat (some are electronically controlled) and home security systems to see if they are Y2K compliant. If not, either learn how to manually override the system or replace them with one that is Y2K compliant.

❑ Prepare for inconsistent services of heat, power, phone, water, food supply, and prescriptions.

❑ Contact the maker of your personal computer and ask if your make and model of computer is Y2K compliant. Even if the manufacturer says the computer is Y2K compliant, be sure to back-up any data on your computer at least 24 hours before the year 2000 date changes.

❑ If you have any medical equipment that is digital, check with the manufacturer for Y2K compliance. (Often major companies have web sites that will list their products and if they have been tested for Y2K compliance.)

Personal and family preparedness:

Prepare as you would for a natural phenomenon, such as ice storms, tornado, earthquake, and power outages. For most natural disasters, you are encouraged to prepare for 3 days without most government or commercial services. This includes utilities, pharmacies, grocery stores, gas stations, banks, etc. Because there is no way to fully anticipate the impact of the "millennium bug", you may want to consider extending your preparedness plan for 7 days.

❑ Water
- One gallon per person, per day for 3-7 days
- Purifying agents

❑ Food
- Ready to eat canned meats, fruits and vegetables
- Soups, Canned milk, Juices
- Stress foods like canned pudding, cookies and hard candy
- Staples like sugar, salt & pepper
- High energy foods like peanut butter, nuts, trail mix, etc.
- Manual can opener
- Something to heat water safely with, like a small camp stove

❑ Non Prescription Medications
- Aspirin or non-aspirin pain reliever
- Antacid
- Laxative
- Anti-diarrhea medication

Mr. HORN. That's a fascinating presentation. This is the first time I've heard of fifth graders involved, and I think it's a terrific idea. And a number of cities are trying to use their billing method and everything else to get messages, but if you hit all the citizenry, that, too, is amazing.

Now, what I'd like to ask is one or two questions, then I'm going to ask my colleagues to do it. And staff will go around and get your written questions, and we'll work those into the dialog. And then Mr. Willemssen will close out the dialog based on what he's heard this morning.

So let me begin. And we'll start with Mr. Hedrick and all of you. I'd like to go down the line. You've been immersed in this for a number of years, each of you.

I've said from the very beginning this is a management problem, not a technological problem. Sure, we use this or that, experts in computers and whatnot. But now that you've been through this, if you could do it over, what would you do that you didn't do? And you sort of might have stumbled into it like everybody else has stumbled into it.

So what would you contribute to us, Mr. Hedrick, on what relates to you, that you wish you had done 2 or 3 years ago?

Mr. HEDRICK. Well, I agree with you that this, at the very beginning, was a technology issue and rapidly evolved into a management issue. And we've actually learned some very good lessons in State government about how to manage complex problems that we're adapting for some future use.

For example, our group of deputy directors at State agencies has met twice a month to assess our progress on Y2K, and is now continuing to meet twice a month to map our progress on building more digital government and electronic commerce.

If we had to change something, I think we would have looked at the problems of embedded systems earlier than we did. As I mentioned in my testimony, we've been looking at our IT systems for 6 years now, and those are complete, essentially. Our embedded systems, though we've found fewer problems than perhaps we expected, we had to address more rapidly than we probably should have.

Mr. HORN. Mr. Burwell, any suggestions, now that you've gone through this exercise? What would you like to have done over, earlier?

Mr. BURWELL. Well, I think one of the things would be, again, the embedded systems. We didn't really understand the impact and how to test those.

I think one of the things we found early on, we were treating it like just a technology problem, and clearly it wasn't. And I think we would get agency involvement from the business side involved earlier. When we started our process, we were really working technology with LAN administrators, et cetera, not the people that knew the business and what were really the essential services.

I think early on, also, we would have shifted the emphasis from resolving and fixing PCs and desktop equipment. That was our easiest job. That was absolutely the most easy job. It was dealing with applications and vendors and that sort of thing. And so we would have addressed that sooner on in the project.

And finally, we weren't prepared to deal with and archive and index the volumes and volumes of information that my office was getting from the agencies. And that can be a real benefit in getting that information from all of the agencies and it becoming the base for a business and a technology inventory.

Mr. HORN. Mr. Chakoian.

Mr. CHAKOIAN. I certainly agree with what my colleagues have said. I guess I would answer the question a little bit differently in terms of what have we learned that we can now institutionalize? What are the lessons we have learned that can become part of our way of doing business?

And certainly having a better understanding of the relationships between our applications and the business functions that they serve; keeping business people more closely involved in decisions about the computer systems; standardization has been a big boon for us; really learning how to do good testing, we need to make that part of our way of doing business; and contingency planning.

I think we have made huge strides in having good contingency plans in place that will not only serve us for Y2K, but for any kind of problem or emergency that we face. So all of those things need to become part of our way of doing business.

Mr. HORN. Ms. Graff, if you had to do a few things over, what would they be?

Ms. GRAFF. One of the easiest things about preparing for Y2K was the fact that we already had an all-hazard emergency operations plan for the city in place. Therefore, what we did for this specific threat was simply take a close look at our planning assumptions to figure out what's different about this event than any other regional disaster, such as an earthquake.

I think what we would have done differently, had we had the opportunity, was lobby for exactly the actions that Congress took, which actually led the way to more businesses and entities sharing information with each other, rather than under the incentive of watching out for a lawsuit, trying to keep themselves in business. And those are the kind of partnerships that prepare any type of region or single entity for a disaster. Hopefully, like Marty mentioned, we'll learn and carry into the future some of the benefits of how we prepared for Y2K.

Mr. HORN. Let me now yield to my colleagues here, and start with Ms. Dunn, on any questions she might have of the panel.

Ms. DUNN. Let me just ask Mr. Willemssen a question off the top, because you caught my attention, Mr. Willemssen, when you talked about the Social Security Administration and you said that there is some work, minimal work, that remains to make sure that the Social Security Administration is fully ready.

Can you tell us what that work would be?

Mr. WILLEMSSEN. I testified approximately 2½ weeks ago on Social Security, and the testimony touched on Y2K.

Among the areas that SSA still had to work on is one of their mission-critical systems had not yet been certified as compliant. Second at that time, they had approximately six data exchanges with outside entities that had not been fully tested and certified.

Third, SSA was using a quality assurance tool, after everything had been remediated and tested and implemented, as a doublecheck to see if there were any problems that could be identified with this independent quality assurance tool, and they did find some problems that they are now following up on.

And finally, another key area was that SSA had still remaining testing of their key contingency plans that they had to do.

So there were a number of remaining tasks, but I'm confident that they'll get them done, because one thing that has been very evident among the Federal agencies is that Social Security is the leader. They've been very responsive to us whenever we've raised issues, and they immediately take action to address those issues.

Ms. DUNN. Thank you very much. That's good to know.

Let me ask a question of Mr. Hedrick. We recently read that three States are now Y2K compliant. You say that 98 percent of our State computer systems are fully compliant. How long will it be until we become a member of that wonderful list of only three now?

Mr. HEDRICK. There are six State agency computer systems that have some testing remaining to do that will be completed over the next 6 weeks.

We also, as part of the auditing and assessment process, have looked at the status of higher educational institutions in the State, and there are a couple of those that have systems that will be completed over the next 6 to 8 weeks, also.

Ms. DUNN. Thank you very much. I wanted just to mention to Ms. Graff, because your city is part of my district, and I'm very proud to represent more than half of Bellevue, I liked your comment about Seattle being the restaurant community for Bellevue. That's pretty appropriate these days.

In the work that you are doing on behalf of the city, have you run into problems of fear of liability from companies that you've been dealing with? Is this what you were saying to us earlier?

Ms. GRAFF. Not as much fear of liability as generic apathy to get ready for any type of disaster. In other words, they're in about that third phase of denial, that this really won't be that bad.

And we'd just as soon that they would treat it in such a way that this might not be that bad, but the earthquake will be. Get ready once and you're ready for everything.

So I wouldn't say that there's too much of that negative kind of energy on the local level from the businesses that we've talked with or the Chamber or the Bellevue Downtown Association, but it's a matter of getting their interest level up to do something.

Ms. DUNN. Good. Mr. Chakoian and Mr. Burwell, I wanted to just ask you, as you have been so involved in organizing this for King County and Seattle, what are you most fearful of? Is there some area that comes to the top of your mind if you were asked what are you worried about? What are you worried about maybe for your families or your community as we move toward Y2K?

Mr. BURWELL. That's a good question. And I get that question an awful lot from friends and family and colleagues. My biggest fear is really the public hype and what's going to happen if you see your neighbor buying extra loaves of bread or filling up every vehicle and going to the bank and that sort of thing, and that we have to deal with with education.

But that's my fear, more than the technology or power outage or that sort of thing, is having to deal with citizens overdoing it and not being educated. That really, this is just like—treat it like a storm, a three to 5-day storm, not a Seattle storm of one flake of snow, but a Chicago storm where you might be without transportation for 3 or 4 days.

But to me, it's what I'm calling the public hype that I'm worried about, that things might get exaggerated. We've heard rumors of possibly a couple of movies coming out the last quarter of this year, and what is that going to do to the public minds? So that's my concern.

Mr. CHAKOIAN. Other than the long-term economic factors, which I've already mentioned I'm concerned about, I think in the short term, I have to agree with Clif. We will be ready to operate as normal. It will be a normal time for us because we'll be prepared. And if the public behaves normally, then we'll all get through this fine.

If everybody picks up the phone at the stroke of midnight and calls 911 to see if it works, it won't work because the lines will be jammed. But if everybody acts in a normal, responsible way, I think we'll be fine.

Ms. DUNN. Thank you. So as one of the members of our audience, Mr. Lloyd Robbins, has said in a question that I would submit to be asked later, he has said that we must be able to provide the public with adequate assurance that any possible problems after January 1, 2000, will be minimal, and that this will be quickly corrected. Thank you.

Mr. HORN. The gentleman from Washington, Mr. McDermott.

Mr. MCDERMOTT. Thank you, Mr. Chairman. It's always heartening to hear that everything is perfect and it's going to work well. And I've been around long enough to always wonder if that's exactly true.

Are there any systems at either the State or city or county level that you think are liable to fail in this period? Important systems, let me make that clear, because one of the systems you said you were still working on was the distribution of ball fields. And I'm not sure, on January 1st, how important whether or not you can get the lights on at the Queen Anne Community Center to play soccer is. So I'm talking about important systems.

Mr. CHAKOIAN. Well, the parks department considers that an important system. It is on their mission-critical list, and it will be ready by January. But other systems also will be ready. There is no system on our mission-critical list that I can think of that I'm particularly worried about.

On the other hand, we'll have contingency plans in place in case any of our external interfaces don't work. So if there's a problem with any of our vendors or suppliers, we'll have work-arounds for that.

So I'm not saying today that everything will be perfect, but I am saying we'll be ready for whatever happens. And the mayor has given us the charge of ensuring that there is no disruption in basic service to the public, and we will honor that and we'll achieve it.

Mr. MCDERMOTT. King County?

Mr. BURWELL. Well, I am worried. I'm confident, and I feel that we are ready, but I am worried because there are so many variables involved in this project, from the outside, from vendors, from power sources, from interfaces with other systems, our systems with the State of Washington, et cetera, and anything can cause a problem.

But I'm confident in that we can fix the problems. We have contingencies. We have backups. We have test plans for the actual rollover weekend. And I've been in this business a long time, and we're good at solving problems quickly, if there are problems. And like Marty from the city, we don't expect problems. We think we're prepared. But there's probably going to be some problems, but we're prepared to fix them quickly.

Mr. MCDERMOTT. The State?

Mr. HEDRICK. We've identified over 400 mission-critical systems. Every single one of them is going to be fixed and tested. But we live in a very interdependent environment where it is impossible to test every conceivable interface with other data, for example, from the Federal Government, but we will ensure that we meet the government's goals of no interruptions in service or loss of accountability.

But we've established very detailed contingency plans. As other panelists have mentioned, this has been a great opportunity to do contingency planning that we should have been doing in any case and have been doing in any case, but have improved a number of those contingency plans that will be useful in the case of any disruptions.

Mr. MCDERMOTT. One of the things that troubles me about this whole business is you all mention vendors, the interface between government and the vendors. And what's a little bit troublesome to me was Congress passing a bill giving blanket freedom from liability to vendors. And because that takes the pressure off, it seems to me, to get up and get running, exactly what was suggested by Ms. Graff, that some people say, "Well, it's not going to be much of a problem. No problem, we'll fix it by and by."

I wonder to the extent of what vendor areas do you see as the most difficult ones where you interface with the vendors from the outside? What are the most difficult ones?

Mr. CHAKOIAN. I guess I'll take a crack at that. We've identified 396 key vendors and suppliers that the city of Seattle depends on, and we're contacting those one by one and going through with them, trying to ascertain what is their year 2000 program, how are they doing, what level of confidence do we have of them.

And so far, those discussions are going very well. Most of the companies that we deal with are larger companies that have the resources, and so on, to do the same kinds of things that we're doing.

What does concern me is not that somebody won't be in business the first couple of weeks in January, but that overall, the worldwide connectivity of suppliers and products that these vendors depend on in the long term could have an impact.

So I don't expect to see anything in January or February where a company that we depend on can't do business with us. I'm concerned about, over the first 6 months, seeing some of our key business partners perhaps have some difficulties based on their international dependencies.

Mr. BURWELL. Without getting specific on a specific vendor, vendors and ourselves are reluctant to use the word “compliant.” We’ve been advised by our prosecuting attorney not to use that word; “We’re Y2K-ready,” or, “We will be Y2K-ready,” again, because there are so many variables.

And so that’s kind of how we answer questions about our state of readiness, that we’re trying to avoid the word “compliant.”

But I’ve found with some vendors, one in particular that I would rather not mention, that is so reluctant that they won’t give us a status, and we have to go to sources like the web and those kind of things to get information, but is one pretty critical vendor who we believe is ready but will not give us any statement of readiness.

Mr. MCDERMOTT. Is that a liability question, a legal question? They don’t want to set themselves up having said, “I’m compliant,” and then it turns out that——

Mr. BURWELL. I think it is. I think it is. And just recently I got a phone call, and it was a recorded message from a vendor, and it went on for minutes, what they will and what they won’t do, and if you do this and if you don’t do this, and blah, blah, blah, our product is not ready.

And it was a very disappointing statement to me that a vendor would announce their readiness, or lack of it, via a recorded phone message.

That’s just kind of two examples of what I’ve faced, but there’s a reluctance by many to say “we’re compliant” because of the variables and outside influences on their ability to be compliant. So they’re reluctant to communicate that.

Mr. MCDERMOTT. At the State level?

Mr. HEDRICK. We have tested every vendor-related information technology issue. But State government is dependent upon a wide variety of vendors, from the buildings that we lease—and we’ve asked for Y2K assurances on all of those—to, for example, foster care and health care that State government contracts for.

We do not have the capacity, for example, to independently audit every single one of the Y2K statuses of all health care providers in this State which we regulate and, in many cases, are vendors because we pay bills.

Our Department of Health has sent letters to every single health care provider that we regulate and demanded assurances that they’re dealing with the Y2K problem, and let them know that they’re going to be responsible for carrying out their responsibilities come the beginning of the year, and demanding a response back.

And one of the interesting things that we’ve done is, last week, we released on the World Wide Web and to the press the names of every hospital, for example, in the State that sent us back the letter, and every one that didn’t. And that got their attention pretty quickly once that was released.

So again, it goes back to our fundamental belief that we need to provide the public with as much information as possible, and that people will make good decisions based upon that good information. But we live in a world of uncertainties.

Mr. MCDERMOTT. I didn’t mean to exclude Bellevue. Have you had problems with vendors?

Ms. GRAFF. We're pretty much in the same boat as Seattle is, that it's very difficult to get a clear compliancy statement from absolutely all of our vendors. A lot of us are in this form-letter chain system right now where they send us a form letter, we send one back, we send a more complicated one, they send a more complicated form letter back.

I think that one of our biggest concerns, quite frankly, are the testing procedures that still need to be done throughout the remainder of the year. I think we're all aware of the fact that unless you have the folks from the vendors or the manufacturers available to help in the testing procedures for equipment that has microprocessors or microchips, you may well invalidate the warranty associated with that equipment.

And I think that more and more people who are just now getting to the testing phase, and if their schedule is perfect and nothing interrupts them and there's enough technicians to go around, they'll say, "Yes, we will be done by such and such a day later this year," whether or not there's actually enough folks to go around to do that. So I still have a little caution about the testing procedures.

Mr. MCDERMOTT. Thank you, Mr. Chairman. I think it's an issue that we need to look at carefully in terms of what kind of liability exclusion we give people.

Mr. HORN. Let me just ask a brief question, just because it comes up in different cities and counties and States. In the case of State prisons and in the case of county jails, those systems, in terms of releasing people, we've found in a couple of cases that they had real problems with that regard. And I'm just curious what the jail and prison situation is?

Mr. HEDRICK. All of our correctional institutions are fully compliant.

Mr. HORN. So you won't be letting people out that shouldn't be out?

Mr. HEDRICK. The default is to close the doors, not to open them.

Mr. HORN. How about King County?

Mr. BURWELL. I heard the default was to open the doors.

But in King County, our adult detention facilities, including the Regional Justice Center in Kent, are all Y2K compliant. And we have very strong contingency plans for recovering if there are any problems. But they've all been tested and are Y2K-ready.

Mr. HORN. I want to get in the audience questions very rapidly. So one of them here is: would the Y2K problem affect the stock market?

The answer is: they're OK. Back in our first hearing in 1996, they were working on this. They have done extensive testing in terms of the stock exchanges, and there's no problem there. There's no problem with the clearinghouse. There's no problem with the banks. I talked to Chairman Greenspan 4 years ago on this, and he delegated it to Mr. Kelley, one of the governors, and the banks are in great shape, basically. So we don't have to worry about that one.

And then: what's the status of the Health Care Financing Administration? And my colleagues have an interest in that because that relates to Medicare and Medicaid.

And we do have a problem with some of the fiscal intermediaries, and we will be holding another hearing on that. But they have a very able administrator, and I think she's going to be on top of it. But it is a major problem without a question there.

Mr. Willemssen, do you want to add something to that?

Mr. WILLEMSSEN. Just to concur with your statement. The Health Care Financing Administration and Medicare remain one of the highest-risk Federal agencies. HCFA is busily working at Y2K, and also busily working at the contingency plans in the event that there are disruptions.

Mr. HORN. Now, here's a question for Mr. Burwell, that organizations such as the city of Seattle have been working since 1993 to 1996, and have reached 80 to 88 percent compliance, says this individual in the audience. How can they fix the remaining 12 to 20 percent in 90 days, at least by the end of September?

Mr. BURWELL. I guess that was addressed to me, even though they were mentioning the city.

For King County, we're at about 88 percent right now of our mission-critical systems. Where we're waiting is basically for vendor systems that are replacing noncompliant systems. Those systems are installed and being tested. So we really don't feel there's a problem with reaching that.

Mr. HORN. But that was the question the person had. You've said 88 percent, and they were wondering how you get the remainder, and would you be able to do it in a timely way, either in the city or the county?

Mr. BURWELL. And we would, because it's just a matter of installation.

Mr. CHAKOIAN. It's the same with the city of Seattle. It's not like we're now starting on those remaining 20 percent of the systems. In fact, much like King County, we've already purchased the software. It's been installed. It just hasn't been put into production yet.

Mr. HORN. Does either the county or the city have a hospital that's a public hospital?

Mr. BURWELL. Yes. We support, at least in part, Harborview.

Mr. HORN. Now, the emergency rooms have been one that we've had a lot of testimony on. And when we were in Cleveland with the Cleveland Clinic, which is one of the top hospital facilities in America, they talked about the World Wide Web system that all hospitals can access in terms of manufacturer, manufacturer's model, date of this equipment, and so forth. So they don't have to reinvent the wheel, nationwide. The information is there from the contractor and manufacturer, as well as the hospitals.

So I just wondered if you were making use of that?

Mr. BURWELL. I'm not personally—the University of Washington is overseeing the medical programs there and at Harborview. And I apologize. The only thing I can respond to is that I've heard them say at our stakeholder meetings that they are Y2K-ready.

Mr. HEDRICK. Those are actually state-funded institutions. The University of Washington Medical Center, as part of our assessment process, have gone through our outside auditing process and they are ready. They had some problems early on, but they've resolved those.

Mr. HORN. Here's a question, and Mr. Willemssen, I'll let you answer that one. Please define "Y2K-ready" and "Y2K compliant." Are they the same?

Mr. WILLEMSSEN. No two people will give you the same answer on that. I think it was touched on, I believe, by Mr. Burwell a little bit earlier, about, that generally speaking, the term "Y2K-ready" is held in a bit lower level of stature, and "Y2K compliance" is considered a more difficult standard to achieve.

But in order to really understand those terms, you've got to get to the actual definitions and exactly what the vendor, in this case, is referring to by that particular term.

Mr. HORN. Here is one really for all. Are there score cards or report cards for other municipalities and internationally? Are there these cards?

The answer is no. It's simply been our subcommittee's view that, working with the General Accounting Office, we could translate all the gobbledygook of the quarterly reports and sort of give a view to the Nation, because we're all familiar with grading.

And this is not a pass/fail thing. We actually have worked out between the "Fs" and the "Ds", and the administration as a whole has gone through "Ds", "C-minuses", "C-pluses". They're now at "B-minus". We're confident they'll get to the "A" in a bit.

And the State Department, which was mentioned a little while ago, the State Department is particularly interesting. We've given them "Fs" consistently for several years. And then finally, they moved from "F" to "A minus". And one of the computer newspapers said to one of the supervisors there, "How did that happen?" And the supervisor said, "I guess my boss just got tired of having them give me 'Fs.'" And so it's the last-minute student that's very bright and works all night and finally gets it.

So the State Department has been in that situation. And, of course, the problem there is a lot of interconnections. Not as many as we think abroad, because they are pretty much self-contained in a lot of their computer systems.

But we have a major problem in terms of developing nations. And the World Bank, I had asked 3 years ago for the Secretary General of the U.N. to put an international conference together. They finally did a year ago, and 120 nations showed up. And Mr. Koskinen and I both went up for that one, and it was really an excellent dialog.

And just recently, the U.N. again held a meeting, and as I remember, 173 nations showed up. The World Bank picked up the tab for a lot of this. So it's a last-minute bit, but we have real problems in some of the developing nations in this regard. And a lot of that relates to our trade, to businesses. And if businesses in certain countries can't connect—especially with your great port here—with their subsidiaries in the United States or in Europe, we have problems. And so that's still an open matter.

Then one question was: how do we safeguard ourselves against opportunistic groups that want to take advantage of Y2K failures?

That's a very good question. There will be a lot of nuts that come out of the woodwork, and they'll want to scare you out of the whole building, and you need to not bite. And this was said very well by Ms. Graff. You look at it as just a regular emergency. In the case of California, I think about earthquakes, think about fires, think about floods. We have all of them. And so do you in many ways.

And we just have to systematically be prudent and say, “Keep a little bit of food around.” When I tell my Mormon friends, “Gee, we ought to have at least a couple weeks or couple months,” they say, “Look, we’ve been doing a couple of years forever. So don’t worry about us.”

But that said, just be prudent and get a battery supply and all the rest of it. So I wouldn’t worry on that if we, as was said, use common sense. And that’s important.

And then Mr. Willemssen; could computers that read 2000 as 1900 cause problems? How severe?

That’s the problem. I don’t know what else we can say to it.

Mr. WILLEMSSEN. That’s the subject of today’s hearing.

Mr. HORN. Exactly.

In your written statement, they said to Mr. Willemssen, that the Federal Office of Management and Budget established target dates for agencies to complete business continuity and contingency plans. Has OMB implemented your suggestions? Why or why not?

Mr. WILLEMSSEN. They have not implemented our suggestion of establishing specific dates on when the business continuity plans need to be tested, which we recommended those plans be tested no later than September 30th.

It’s one thing to have a plan on a piece of paper and put on a shelf, but you have to test the plan to make sure that it’s actually going to work should some of these risks realize themselves.

We’re not aware, as of right now, that OMBL, established that date. We know they are putting a lot of emphasis in the area of contingency plans, but essentially leaving it up to the agencies to determine when they’re going to test.

Mr. HORN. I might add that with OMB, when Dr. Raines was director—that’s one or two directors ago—he did a first-rate job in taking over on an attempt at the reporting. And the key there is what some of you mentioned. We’ve had outside verification.

Well, in the case of the executive branch, we asked the inspectors general, which have been created by Congress in all the major agencies, to be that verifier, because when we ask the agencies to produce what are their mission-critical systems, that’s strictly an agency determination, and it’s the right way to go at it because they should know what is most important for them. And I suspect the State looked at it the same way.

Ms. Dunn says Dr. Raines is from Seattle. Obviously, a good person, right? He’s now with Fannie Mae. You can tell he’s a bright person and got out of the executive branch. That’s not said about any administration. It’s just that you can’t beat being at Fannie Mae, and he went there.

The letter of Mr. Robbins and Mr. Bevan of JHB Consulting wanted us to ask this question: who did the independent verification and validation on your systems? And I guess we just go right down the line.

And Mr. Hedrick, who did it in the case of the State?

Mr. HEDRICK. Well, as I mentioned before, we have a two-level system of assessment and auditing. There are a number of different computer consultants that have done assessments at different State agencies and higher educational institutions. A company called Sterling & Associates did the overall risk assessment and this rating.

Mr. HORN. Let me state the rest of the question: if you did your own internal remediation and testing, why didn't you have your software systems validated and verified by an independent, outside organization?

So that's the whole question.

Mr. Burwell.

Mr. BURWELL. And that's a very valid point. And we did do that with an outside consultant, and I hired outside contractors to conduct that IV&V.

Mr. HORN. Mr. Chakoian.

Mr. CHAKOIAN. Yes, we've worked with Data Dimensions to do our assessment, and they're continuing to work with us to do this ongoing audit of our systems and processes.

Mr. HORN. Ms. Graff.

Ms. GRAFF. The city of Bellevue used Coda Consulting, Inc.

Mr. HORN. Well, as they say here, "We hope that your hearings will be able to provide the public with adequate assurances that any possible problems after January 1st, 2000 will be minimal and quickly remedied."

And we thank you all. We're going to have to move to the next two panels, but we really appreciate the dialog here.

Mr. Willemssen, do you have any point in particular before they get up? I'm sorry I didn't call on you sooner, but I wanted to get those questions in.

Mr. WILLEMSSEN. Just one quick point that was mentioned earlier about concern of public overreaction. In my experience, the best way to counter that is by providing, transparently, data on readiness that has been independently verified.

I think you've heard from the witnesses on this panel that they are doing that or plan to do that. And again, our experience shows that's the best way to counter public overreaction.

Mr. HORN. I think you've got it absolutely. Put all the cards on the table.

Thank you, each of you, for coming. A very helpful dialog and very helpful statements. Thanks for coming.

We now will call forward the second panel. And members of the second panel are Mr. O'Rourke, chief information officer, Bonneville Power Administration; Jerry Walls, the project manager for embedded systems, Y2K, at Puget Sound Energy; James Ritch, deputy superintendent, finance and administration, Seattle City Light; Marilyn Hoggarth, manager, Washington State public affairs, General Telephone; Dave Hilmoe, division director, water quality and supply, Seattle Public Utilities; and Brad Cummings, Y2K program manager, University of Washington Academic Medical Center.

Ladies and gentlemen, if you'd stand and take the oath. And anybody who is going to talk behind you stand, too. So I think we've got eleven covered.

[Witnesses sworn.]

Mr. HORN. The clerk will note all the witnesses and their supporters and assistants behind them have taken the oath.

So we will begin, Mr. O'Rourke, with you. And I enjoyed seeing the Bonneville Dam recently. And you are the chief information officer of the Bonneville Power Administration, so we look forward to hearing you.

Mr. O'ROURKE. Thank you, Mr. Chairman.

Mr. HORN. And again, we're talking about summarizing the statement. Don't read it. We've got it. That's automatically in the record right now.

Mr. O'ROURKE. I understand.

STATEMENTS OF JOE O'ROURKE, CHIEF INFORMATION OFFICER, BONNEVILLE POWER ADMINISTRATION; JERRY WALLS, PROJECT MANAGER, EMBEDDED SYSTEMS, PUGET SOUND ENERGY; JAMES RITCH, DEPUTY SUPERINTENDENT, FINANCE AND ADMINISTRATION, SEATTLE CITY LIGHT; MARILYN HOGGARTH, WASHINGTON STATE PUBLIC AFFAIRS MANAGER, GENERAL TELEPHONE CO.; DAVE HILMOE, DIVISION DIRECTOR, WATER QUALITY AND SUPPLY, SEATTLE PUBLIC UTILITIES; AND BRAD CUMMINGS, Y2K PROGRAM MANAGER, UNIVERSITY OF WASHINGTON ACADEMIC MEDICAL CENTERS

Mr. O'ROURKE. Thank you, Mr. Chairman, distinguished members of the House subcommittee. In the role of chief information officer, I am responsible to the administrator for BPA's Y2K readiness. We appreciate the opportunity to appear today, and I appreciate your continued support for this important issue.

Let me get right to the bottom line. Bonneville is confident that our system will operate safely and reliably on New Year's Day, 2000. We are Y2K-ready, and we're confident the lights will stay on.

I don't say that lightly. BPA has taken Y2K very seriously. We're keenly aware of the importance of the power system to the safety and welfare of the Pacific Northwest. We have a long history of exemplary customer service of providing safe, low cost, reliable electricity, and we don't intend allowing Y2K to affect that.

I'd briefly like to talk today about three major reasons why we are so confident BPA will meet the Y2K challenge. First, we've had a methodical program in place since 1995. Second, we have worked closely with our business partners to coordinate Y2K preparations. And third, we're not resting on our laurels. We continue to monitor our systems and redefine and refine our contingency plans right up to and beyond January 1st, 2000.

BPA is a Federal power marketing agency. We sell about 40 percent of the electrical power and about 75 percent of the transmission service in Oregon, Washington, Idaho and western Montana.

We do not own or operate generating facilities. The wholesale power we sell is generated by 29 Federal dams on the Columbia and Snake Rivers that are owned and operated by the Army Corps of Engineers and the Department of Interior's Bureau of Reclamation, and one nuclear plant owned and operated by Energy Northwest.

We saw early that Y2K was critical. We started an inventory of our systems in 1995, and eventually we inventoried over 700 systems, hardware, software and embedded systems and chips.

We made testing mandatory for mission-critical and mission-essential systems and equipment. Where needed, we remediated, then we retested. Then we subjected the program process and test results to an independent review and verification of findings.

Our Y2K-ready systems are on line now, operating the transmission system. We've already passed two critical Y2K dates, December 31st, 1998, and April 9, 1999. By the time January 1, 2000 rolls around, we will have dealt with a third critical date, September 9, 1999.

Secretary Richardson has called our BPA program an example of just plain hard work. And certainly working with the Department of Energy CIO office and their Y2K management team has helped us achieve BPA's objective and the Department's objective: as of March 31st, 1999, BPA is Y2K-ready.

In our efforts, we've worked closely with our generation partners and Federal dams, the nuclear plant and the Western Systems Coordinating Council, or WSCC, and with our utility customers.

The Corps of Engineers and Bureau of Reclamation both announced they were Y2K-ready March 31, 1999. Energy Northwest announced its Y2K readiness June 30, 1999.

The 107 power systems in the WSCC plan to operate their transmission grids interconnected over the New Year's weekend. The WSCC grid is designed to operate more reliably when interconnected. If load and generation is lost, the generators in the WSCC can help each other stabilize their system. WSCC's Y2K task force is planning operations for critical Y2K dates, and conducting Y2K drills and training.

Since our customers' transmission and distribution systems interconnect with ours, they can impact our reliability. We have inventoried the places where our transmission grid interconnects with theirs and collaborated on Y2K readiness, and, as well, we have emergency communications systems set up with all of our wholesale customers.

Finding, testing and remediating, while important, is only one piece of our program. Contingency planning and clean management is where we're focusing our program at this time. No one can predict the future on January 1, 2000, or even tomorrow. That's why we do contingency planning, because there are no guarantees.

BPA has, for years, been bringing the system back on line quickly, seamlessly, following winter storms and lightning strikes, often when end users don't even know it.

The foundation of BPA's Y2K contingency plan is to operate our system so that we have more cushion over the New Year's weekend. BPA's hydro system actually provides more cushion than a system that uses mostly thermal plants. Hydro power can be brought on and off line quickly in response to changes.

Our partners at the Federal dams will also be prepared to operate on manual controls. So dispatchers, and BPA's system as well, predates automation. Thereby, our substations can be operated manually.

We've got the components in place. BPA is ready. Our Y2K-ready systems are up and running. Our generation partners are Y2K-ready, and we continue to be vigilant. That's why I can say that we're confident that BPA's power system will continue to operate safely and reliably at all key Y2K dates.

Mr. Chairman, that concludes my testimony, and we'll certainly be happy to respond to any questions or recommendations from the panel on our Y2K readiness program.

[The prepared statement of Mr. O'Rourke follows:]

TESTIMONY OF JOE O'ROURKE

CHIEF INFORMATION OFFICER

BONNEVILLE POWER ADMINISTRATION

UNITED STATES DEPARTMENT OF ENERGY

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION,

AND TECHNOLOGY

UNITED STATES HOUSE OF REPRESENTATIVES

AUGUST 17, 1999

INTRODUCTION

Mr. Chairman, distinguished members of the House Subcommittee, my name is Joe O'Rourke. I am the Chief Information Officer at the Bonneville Power Administration (BPA), responsible to BPA Administrator Judi Johansen for BPA's Y2K readiness. We appreciate this opportunity to appear today at this field hearing on Y2K, and applaud your continued support and attention to this important issue.

Let me get right to the bottom line. BPA is confident that our system will operate safely and reliably on New Year's Day 2000. We are Y2K ready, and we are confident the lights will stay on.

I don't say that lightly. BPA has taken Y2K very seriously. We recognize how pivotal our system is to the safety and welfare of the Pacific Northwest. We have a long history of exemplary customer service and of providing safe, low cost, reliable electricity. We don't intend to allow Y2K to affect that.

BPA'S MISSION AND FUNCTION

BPA is a federal power marketing agency that sells electric power and transmission service to public utilities, municipalities, cooperatives, industries, and investor owned utilities in Washington, Oregon, Idaho and western Montana. We do not own or operate any generating plants. The wholesale power we sell is generated at 29 Federal dams on the Columbia and Snake Rivers that are owned and operated by the U.S. Army Corps of Engineers and the Department of Interior's Bureau of Reclamation and one nuclear plant, owned and operated by Energy Northwest. We supply about 40 percent of the power used in the Pacific Northwest.

BPA owns and operates about 75 percent of the region's transmission grid. BPA's transmission system in turn is interconnected with 30 other control systems in the Western Systems Coordinating Council (WSCC). WSCC is one of ten independent reliability councils in the North American Electric Reliability Council (NERC). It encompasses the 14 western states and parts of Canada and Mexico that make up the western grid interconnection. The western grid operates independently of the other two major grid systems in the U.S. -- the Eastern interconnection and the Texas interconnection.

Because BPA has primary responsibility for the transmission system, a substantial focus of our Y2K efforts has been on transmission equipment and systems, control centers, substations, and the like. Our generation partners at the Federal dams and Northwest Energy's WNP-2 nuclear plant have had lead responsibility for the generation portion of the power system, and they, too, have announced they are Y2K ready. We have coordinated closely with our generation partners throughout the phases of our respective Y2K programs. In the electric power business, generation and transmission are interdependent, and the reliability of one depends on the reliability of the other.

BPA HAS HAD A METHODICAL Y2K PROGRAM IN PLACE SINCE 1995

Today I want to tell you about why I am confident that BPA will meet the Y2K challenge. I will cover three major points. First, BPA has had a methodical Y2K program in place since 1995. Second, BPA has worked closely and successfully with its many business partners to coordinate Y2K preparations. Third, BPA is Y2K ready, but by no means are we done. We will continue to monitor our systems and refine contingency plans, run drills and tests right up to and beyond January 1, 2000.

We saw early that Y2K was critical, and we got to work -- long before the media attention or consumer pressure stimulated interest in Y2K. We started an inventory of systems in 1995. Then, BPA went through the five familiar Y2K steps: inventory, prioritize, evaluate, remediate and retest and evaluate.

In the process, we inventoried over 700 systems: hardware, software, and embedded chips. We prioritized our testing and remediation according to the impact the system or equipment would have on power system operations. We made testing mandatory for mission-critical and mission-essential systems and equipment. Where needed, we rewrote code, or replaced or upgraded whole systems or parts of systems. Then we re-tested. Then we subjected the program, process, and test results to an independent review and verification of findings.

BPA did its Y2K testing and remediation with in-house staff. We believe this has served us well in a couple of regards. First, BPA employees built many of our own computer software systems, and BPA employees constructed the transmission grid. We are the foremost experts on what's there and how it works, and we applied that knowledge to finding and fixing Y2K issues.

We realized a second, if unexpected, benefit. Recently the report from the Gartner Group revealed some computer software changes where outside Y2K programmers leave open "trap doors" that allow them to continue to access or cause problems for the companies' operations after Y2K work is complete. Any potential security problems were greatly reduced by using in-house staff.

Our Y2K ready systems are on-line now, running the power system. Department of Energy (DOE) Secretary Richardson called BPA's Y2K program " . . .a superb example of commitment and just plain hard work." And we met the Department of Energy goal: As of March 31, 1999, BPA was Y2K ready.

BPA HAS WORKED CLOSELY WITH OUR BUSINESS PARTNERS ON Y2K

The electric business is an interconnected one. Electricity starts at the generating plant, goes to high voltage transmission lines, steps down to lower voltage at substations, and from there goes to distribution systems, where it is delivered to the homes, businesses, and farms that use it. Along the way, plant operators, power marketers, transmission operators, and local utilities work together every day -- across numerous utility boundaries and thousands of miles of transmission lines.

BPA's business partners are legion, but the principal coordination points for us on Y2K have been our generation partners at the Federal dams and nuclear plant, power systems in the WSCC, and our utility customers.

The Corps of Engineers and Bureau of Reclamation both announced that they were Y2K ready on March 31, 1999. Energy Northwest announced its Y2K readiness June 30, 1999. Together with these partners, BPA has prepared Y2K contingency plans, conducted joint Y2K testing, and shared Y2K testing results and information. We have closely monitored their preparations.

WSCC is in an excellent position to coordinate Y2K planning among its widespread and diverse membership. The 107 WSCC member systems have worked together for years to keep power safe and reliable on the western grid. WSCC's Y2K task force is planning operations for critical Y2K dates, conducting Y2K training and drills, and focusing on communication among the Security Coordinators. Security Coordinators are responsible for the reliable operation of the power system within large regional areas.

Member systems in the WSCC plan to operate their transmission grids interconnected over the December 31, 1999, through January 1, 2000 transition. The WSCC system will be postured for conservative operations, which we believe is the most reliable strategy to handle unexpected occurrences. The WSCC grid is designed to operate more reliably when interconnected. Loads and generation can be balanced from one system to another. If load or generation is lost, the generators in the WSCC can help each other stabilize their systems.

Our utility customers are very important to BPA's Y2K efforts. They depend on BPA's reliability for their own customer service. We have provided information and support, including Y2K test results and findings that they can use with their own equipment. We have established back-up communications with them for the transition into the year 2000.

Since our customers' transmission and distribution systems interconnect with ours, they can impact our reliability. We have inventoried the places where our transmission grid interconnects or interacts with theirs, and other related businesses -- at power plants, adjacent transmission grids, and customer substations – and we are collaborating with them on Y2K readiness.

On the national level, BPA is a key player in the nationwide Y2K drills sponsored by NERC, which has played a major role in Y2K planning for the utility industry and working with the Congress and the Executive branch of the Federal government. The first NERC drill, on April 9, 1999, was deemed an overwhelming success, meeting objectives while revealing minor adjustments that can be made in systems and training.

We are eagerly anticipating a visit from Secretary Richardson on September 9 to participate with BPA and the Pacific Northwest in the second NERC drill. This one will test the contingency plans developed for Y2K and serve as a "dry run" for New Years Eve.

BPA WILL CONTINUE TO PREPARE FOR Y2K RIGHT UP TO AND BEYOND JANUARY 1, 2000

We're proud of our Y2K results. But we're not resting on our laurels.

Finding, testing, and remediating, while hugely important, is only the first part of BPA's Y2K program. "Clean management" and Y2K contingency planning will continue right up to New Years Day...and beyond.

Clean management refers to our ongoing Y2K monitoring of systems and equipment. BPA acquires new components, updates systems, and repairs equipment continually in the line of maintaining smooth and reliable operations. With every change, we retest each system for Y2K readiness. We're including provisions in many of our software or hardware contracts for Y2K readiness disclosures. Between the dates of November 15, 1999 and January 15, 2000, we will freeze implementation of new embedded system equipment and computer hardware and software.

Contingency planning isn't new to us. Like any electric utility that's been in the business for more than 60 years, BPA has lots of experience planning for unexpected events. Winter storms, lightning and cold snaps happen every year. For years, we've been bringing system components back on line quickly and seamlessly following power disruptions, so that end users don't even notice.

Of course no one can predict the future – on January 1, 2000 or even tomorrow. We do contingency planning precisely because there are no guarantees. We anticipate a range of likely outcomes and then make timely and thorough preparations for them.

The foundation of BPA's Y2K contingency planning is to operate our system so we have more "cushion" over the New Year's weekend going into the year 2000. This means we operate conservatively, have back-up systems, more power and transmission in reserve, and more staff on board.

BPA's hydro-based system actually provides more cushion than a system that uses mostly thermal plants. Hydropower is more flexible. Hydropower plants can be brought on and off-line quickly in response to changes. Because it can be available more quickly, hydropower is also a useful back-up if any other generation is lost. The Corps of Engineers and the Bureau of Reclamation at the Federal dams will also be prepared to operate on manual controls should the computer-based generation control systems be lost. Energy Northwest has also developed a plan for the roll over date that will position the WNP-2 nuclear plant to respond to unplanned events.

BPA's own transmission system also pre-dates automation, so dispatchers and substation operators can run it manually. BPA has also installed a satellite telephone system that will back up its several other communication systems, most of which operate independently of the public telephone system.

BPA and the generating plant operators will have more staff than normal at work and on call at the control centers and substations during the December 31, 1999, to January 1, 2000, Y2K rollover. WSCC Security Coordinators will contact each of the control centers on a regular basis and share information with the others. NERC will have a system in place to quickly transmit the real-time experiences and actions from earlier time zones to utilities in North America and their affiliates in other parts of the world.

CONCLUSION

On August 3, 1999, NERC released its fourth quarterly report to DOE on electric industry Y2K readiness. In it, NERC said that more than 99 percent of mission-critical systems and component were Y2K ready, and that the electric power industry will operate reliably into the Year 2000 with the resources that are Y2K ready today. NERC listed BPA among the 251 bulk power suppliers (of a total of 268) that are Y2K ready.

We believe NERC's report is testimony to the seriousness with which our industry has approached Y2K. For our part, BPA is keenly aware of the importance of the power system to this region's economy and welfare. We have been entrusted with a crucial responsibility. We are intent that Y2K not jeopardize our track record of reliability and customer service.

And we've put the key components into place. BPA is Y2K ready. Our Y2K ready systems are up and running. Our generation partners are Y2K ready. We continue to be vigilant.

When New Year's Eve 2000 rolls around, we will have already encountered and dealt with at least three critical Y2K dates – December 31, 1998, April 9, 1999, and September 9, 1999 -- two of which we've already passed without disruptions in service. Contingency plans will be in place and ready. We will have participated in two North American power system drills.

That's why I can say we are confident that BPA's power system will continue to operate safely and reliably on all key Y2K dates.

Mr. Chairman, thank you for this opportunity to appear before you today. This concludes my formal testimony. I would be pleased to address any questions or suggestions you may have regarding BPA's Y2K readiness.

Mr. HORN. That's very helpful information. And we'll wait until we're all done, and then we'll have the dialog and questions.

Jerry Walls is the project manager for embedded systems on the Y2K project for Puget Sound Energy. Mr. Walls.

Mr. WALLS. Good morning, Mr. Chairman, members of the committee. I want to thank you for inviting Puget Sound Energy here today to discuss our Y2K efforts.

Based in Bellevue, WA, Puget Sound Energy is an investor-owned utility that has served the Puget Sound region for about 100 years. We have approximately 550,000 natural gas customers and 900,000 electric customers.

We began working on Y2K issues approximately 3 years ago. On June 30th of this year, we filed a report with the North American Electric Reliability Council stating that we believe all of our mission-critical systems are Y2K-ready. This conclusion results from both our own internal seven-step approach to Y2K readiness, but also as well as working with our service providers to ensure that they are also Y2K-ready. In addition to our electricity operations, our gas operations also were Y2K-ready by our June 30th deadline. And we believe that on December 31st, 1999, that we will be conducting business as usual in both our electric and gas operation.

Puget Sound Energy conducted a very extensive program to identify and check every component and system. If they found a problem, that problem was remediated and fixed.

As part of that assessment and remediation, we did an extensive amount of testing to ensure that our systems were Y2K-ready. This included, in many of our systems, what we would call an integrated end-to-end test of all of the integrated systems. This is both internal and external to our company.

Our objective, overall, was to learn that our gas operations, our electric generation, transmission and distribution, and telecommunication systems were all Y2K-ready.

Through this $14 million process that we've been going through for the past 3 years, we physically surveyed more than 1,500 sites in 11 counties in the State of Washington. And through that process, we evaluated more than 25,000 separate items for date sensitivity that could have caused Y2K problems.

However, interestingly enough, throughout this process, our Y2K team did not find a single item that we felt would have caused a severe disruption of either our gas or electric systems.

However, working with those systems that either control or monitor our energy systems or telecommunications, we did find Y2K issues, and these would have hampered our operations and caused us to use manual backup systems that we've used in past times. But again, by June 30th, all the problems I just mentioned were Y2K-ready and they've been tested.

In addition to those items I discussed, in our field areas, in the sites we visited, we replaced more than 500 separate devices that were not Y2K-ready. And probably close to two dozen separate computer systems were remediated, to some extent, for those systems that monitor or control our energy systems or our telecommunications systems. Again, in total, of all of the items that we looked at, less than 2 percent of these required remediation.

Beyond the assessment and remediation of our own embedded systems, another important part of our work was contact with our critical service providers of energy and other critical services such as telecommunications. They have reported to us that they are Y2K-ready, and we have confidence in what they tell us.

While we are pleased with our own Y2K initiative, it's important to have backup plans in place. And as we reported to NERC on June 30th, we cannot make absolute guarantees, of course, because Y2K is very complex. However, we have, as part of our readiness effort, a comprehensive contingency plan. Contingency planning is not new to Puget Sound Energy. We have had emergency plans in place for the 33 years that I've worked at this company, and before.

Our comprehensive plan defines what we would think as unlikely Y2K scenarios that could occur on any part of our system. And part of the plan also includes detailed procedures and plans, how we would address any misadventure that could occur during the Y2K period.

The plan includes staffing plans. We have more than 250 people onsite throughout our company, in mission-critical areas in our company, as well as, well before the rollover period, we'll have our Emergency Operations Center open, as we do during any company emergency.

Our contingency planning has also included participation in the nationwide NERC drill on April 9th, which was a telecommunication drill. And we will also participate in the NERC drill on September 8th and 9th. We will be participating in that.

Also, we have internal drills that we will conduct from now throughout the year, as we do every year when we prepare for wintertime.

And with that, Mr. Chairman, that concludes my remarks.

[The prepared statement of Mr. Walls follows:]

"Is Seattle Prepared for Y2K?"
Y2K Readiness Field Hearing
Government Reform Subcommittee on Management, Information and Technology
August 17, 1999
Jackson Federal Building, Seattle Washington

Good Morning Mr. Chairman and members of the subcommittee. I want to thank you for inviting me to discuss Puget Sound Energy's Y2K Readiness efforts.

My name is Jerry Walls. I am the Project Manager for Puget Sound Energy's Embedded Systems, Y2K Project.

Based in Bellevue, Washington, Puget Sound Energy is an investor owned utility that has served Puget Sound citizens and businesses for more than 100 years. We serve 555,000 natural gas customers and 900,000 electricity customers.

Puget Sound Energy first began working on Y2K issues about three years ago. On June 30, 1999 we filed a report with the North American Electric Reliability Council stating that we believe all mission critical systems are Y2K ready, as defined by NERC. This conclusion results from both our own 7-step approach to Y2K Readiness, as well as the Y2K Readiness reports provided by our service providers.

In addition to electricity operations, our natural gas operations also were Y2K Ready by our corporate deadline of June 30. We intend that both our gas and electric operations will be conducting business as usual on and after the Year 2000 rollover.

Puget Sound Energy has conducted an extensive program to identify and check every component and system, and then fix or replace problem items. In addition to equipment Assessment and Remediation, we tested our systems for Year 2000 Readiness. This included conducting integrated, end-to-end tests of all mission-critical equipment and systems. In conducting both internal and external tests, our objective was to learn if all aspects of the gas and electric generation, transmission, distribution and communications systems were Y2K ready.

Through the $14 million Y2K Readiness process, we physically surveyed embedded systems at 1,500 different company locations in all 11 Washington counties we serve. We identified and evaluated 25,000 items for potential date sensitivities that could have caused Y2K problems.

Throughout the project, our embedded systems team found only minor problems. None would have caused severe electricity or natural gas service disruptions.

We did find Y2K problems within some systems that remotely controlled or operated the electric, gas and telecommunications equipment. Had these systems not been remediated, they would have hampered operations of both the electric and gas systems, requiring the use of back-up, manual systems. By June 30, 1999 all of the problems to which I refer were Remediated and Tested.

In addition, we Remediated more than 500 separate devices on the electric and gas systems, and at least two dozen central computers that operate and monitor both our energy and telecommunications systems.

In total, less than 2% of the embedded systems we Identified and Assessed, required remediation.

Beyond the Assessment and Remediation of our own embedded systems, another important part of the project has been our contact with major energy suppliers and service providers to evaluate their Y2K Readiness. They have reported to us that they are Y2K Ready.

As the year progresses, we will continue to monitor our mission critical energy service providers to ensure that they stay Y2K Ready.

While we are pleased with the results of our Y2K initiative, it is important to have back-up plans in place. As we reported to NERC, no company can make absolute guarantees about something as complex as Y2K. As part of our Y2K Readiness effort, we have prepared a comprehensive Contingency Plan that supplements Puget Sound Energy's long-term emergency plans.

This comprehensive plan identifies unlikely Y2K scenarios and includes procedural solutions for the company to follow in the event that service disruptions materialize.

The plan also includes staffing plans for the millennium rollover. For example, approximately 250 employees will be working on site during the rollover, and our Emergency Operations Center will be open.

Our contingency planning includes participation in several nation-wide drills, including one that was held on April 9, and another scheduled for Sept. 8th and 9th.

Mr. Chairman, this concludes my prepared statement. I would be pleased to answer any questions you or other members of the subcommittee may have.

Information contained in this document is a "Year 2000 Readiness Disclosure" in conformance with the Year 2000 Information and Readiness Act of 1998 (Public Law 205-271, 112 Stat. 2386) enacted on October 19, 1998.

Mr. HORN. Thank you very much.

Mr. Ritch. Mr. Ritch is the deputy superintendent, finance and administration branch for Seattle City Light.

Mr. RITCH. Thank you, Mr. Chairman and honorable members. Thank you for inviting Seattle City Light to testify regarding our utility's year 2000 readiness. I'm especially pleased to be here, since it's another opportunity to let our customers know that we are highly confident that our power will not be interrupted by the transition into the year 2000.

In the way of background, Seattle City Light serves over 350,000 customers. In a typical year, we supply approximately 75 percent of our load from our own hydroelectric plants in the northwest. Seattle City Light is the seventh largest municipally owned utility. We are very proud that Seattle City Light offers the lowest cost, most reliable electricity in urban America. It is our mission to give our customers safe, economical, reliable electric service. We take this mission very seriously.

We have taken the Y2K rollover challenge very seriously as well. Seattle City Light has been working to solve our Y2K problems since 1995. In February, Seattle City Light created a central Y2K project office to facilitate Y2K legal review, maintain project records, and coordinate the assessment and remediation testing and contingency planning for critical business functions.

In order to keep track of what's critical, we broke our business into essentially eight critical functions, half of which involved the generation and delivery of power, the other half involved things like billing, payroll, paying vendors, getting materials, et cetera.

On the business application side, we have most of our work force devoted to field operations. These are the people that make sure that the electricity is generated, transmitted, distributed to our customers.

To keep things running smoothly, we use many computers to keep track of materials, schedule field crews, even enter time sheets. Every day, over 100 different field crews head out for work. When we went through our systems, we found that many of these business applications could not successfully process the year 2000 date.

We also need to provide accurate billing and account information services to our customers. Our computer systems generate over 10,000 bills and process over $1 million worth of receipts every day. Early on, we determined that many of these systems also could not get you from 1999 to 2000. These are just two examples of how software works in basically the back office of Seattle City Light.

I'm pleased to report that we have now completely remediated all 16 of our mission-critical business applications. We're now stepping through the city of Seattle's Y2K certification process for these critical systems. And it's important to remember that these systems do not affect our ability to deliver power to our end customers.

On the operations side—and the BPA mentioned how important this is—the system is very interconnected. Seattle City Light has been working with the Western States Coordinating Council and North American Electric Reliability Council in coordinating our Y2K efforts.

In early May, the U.S. Department of Energy asked NERC to assume leadership in preparing electrical utilities for the transition to the year 2000. That was in 1998. June 30th was the date for utilities to have remediation and testing completed for mission-critical systems. And these systems are things like relays, et cetera, that make sure that electricity is delivered.

Only about 5 percent of our electric system's equipment contain embedded systems. For example, of the 5,000 protected relays that are used in our system, only 80 contain embedded systems. The vast majority of our field equipment is made up of electromechanical devices that pose no Y2K failure risk.

Since a lot of the work is, and I think the embedded systems, at least for us, is one of the more difficult ones, we also hired a consulting firm, TAVA/Beck, to go through some of the inventorying that we did to make sure that we captured all of the potential areas of exposure in the embedded systems side. This would include systems at our powerhouses, substations, communications facilities, and our system control center. Based on their work, we are very confident that we have found and remediated those systems that had embedded chip issues.

As of June 30th, all mission-critical generation, transmission and distribution equipment used in the production and delivery of power has been tested, remediated and declared ready for operation in the year 2000 and beyond. In the earlier panel, you talked a little bit about supplier readiness. We did contact over 400 of our vendors, and we got responses back from 90 percent. About half of them said they were Y2K compliant. Another 25 percent said they would be by the end of the year. And the other 25 percent are still trying to figure out how to respond to us. So I think that we are experiencing similar issues.

Just one thing about contingency planning. The nature of the electricity business is that you have to be ready for any kind of emergency, whether it's lightning storms, earthquakes or fires, or what have you. We have well-established procedures in place to make sure that the power, if it goes out, comes back on as soon as possible.

Over the rollover period, we will have staff at our powerhouses and system control centers and elsewhere to make sure that things flow as smoothly as possible.

I guess, finally, we have had our program checked over by an independent quality assurance consultant. We have had very successful results in that, and that reinforces our confidence that Seattle City Light's power will not be interrupted by the transition to the next millennium. Thank you very much.

[The prepared statement of Mr. Ritch follows:]

TESTIMONY
Seattle City Light's Year 2000 Readiness
U.S. House of Representatives
Committee on Government Reform
Subcommittee on Government Management, Information, and Technology
By James Ritch, Deputy Superintendent
Finance and Administration Branch
Seattle City Light
August 17, 1999

Thank you for inviting Seattle City Light to testify regarding our utility's Year 2000 (Y2K) readiness. I am especially pleased to be here since it is another opportunity to let our customers know that we are highly confident that Seattle City Light's power will not be interrupted by the transition into the Year 2000.

In way of background, Seattle City Light became a department of the City of Seattle in 1910 and provided electricity for the City's streetlights. Today, Seattle City Light serves over 350,000 customers in a fairly concentrated service area of 131.1 square miles. This territory includes the City of Seattle, north to the King County boundary, including the City of Shoreline and parts of Lake Forest Park. We also extend south into the cities of Burien, Tukwila and SeaTac. We are a hydroelectric-based utility and have generating plants located on the Skagit, Pend Oreille, Cedar, and Tolt Rivers, and several small plants on irrigation district canals. Some of our facilities are directly connected to Seattle's load centers. Other plants are connected via the Bonneville Power Administration and through other utilities such as Puget Sound Energy. Seattle City Light maintains over 600 miles of high voltage transmission lines that run from generating facilities to major substations. These lines are designed to provide multiple connections to the western power grid. We have 14 major substations and almost 2500 miles of distribution lines. Our load ranges from an average of 1100 Megawatts to a peak of 2300 Megawatts. In a typical year we generate approximately 75% of our load, which helps to keep our rates low. Roughly 1,700 employees serve customers and help steward these facilities. In terms of customers served, Seattle City Light is the nation's seventh largest publicly owned utility. We are very proud that Seattle City Light offers the lowest cost electricity in urban America!

But it's not just our low cost electricity that keeps customers such as Boeing, Nordstrom, the University of Washington and Birmingham Steel content with our services. It is the reliability of those services. It is our mission to give our customers the safest, most economical, and reliable electric services in America. We have a public trust and take our mission, as well as the stewardship of these public properties very seriously indeed. We have taken the Y2K rollover challenge very seriously as well.

Seattle City Light has been working to solve its Y2K problem since 1995. We initially focused our attention on correcting the Y2K problems associated with our critical business systems followed by work in our operational areas. In order to better manage these efforts, the utility's senior management formed a Y2K steering committee in late 1998. In February of 1999 Seattle City Light created a central Y2K project office. The project office is chartered to facilitate Y2K legal review, maintain project records, and coordinate the assessment, remediation, testing, and contingency planning for critical business functions. We have identified eight critical business functions that are evenly split between business and operational areas.

Business Applications
As you can imagine, a utility like Seattle City Light has most of its work force devoted to field operations. Maintaining our electric system so that we continue to provide safe, reliable, and economical power is one of our core missions. The City of Seattle has been fortunate to experience a notable economic boom. New office buildings, hotels, and a state-of-the-art major league baseball stadium have placed greater power demands on our downtown core. Additional engineering and equipment upgrades have been and continue to be required to meet the growing

business needs of our commercial and industrial customers. To keep our field operations running smoothly, it's vitally important that we have the right materials, at the right time, in the right quantities, for the right jobs. Over 100 different field crews of varying size head out for a typical day's work. Like many utilities, Seattle City Light has been using computerized software applications for several years to help us efficiently schedule the work of crews, order and procure materials, and keep our inventories well stocked. Dates are used everywhere in these software applications. When we really started looking, we realized that many of our business applications could not successfully process the year 2000 date.

It is also important that we provide accurate and timely billing and account information to our customers. We use computer systems to generate over 10,000 bills each day. We also use computerized handheld devices to read our meters. There are strict deadlines we have to meet to process over $1 million worth of customer bills each day. If we miss running the day's bills or if we have to re-run bills, it has a terrible trickle-down effect. Balancing one day's revenue has to be accomplished before the next day's bills can be processed. After several days, a manageable irritation can become a fairly serious business situation as tens of thousands of bills stockpile. If the situation goes on for too long, cash flow can become an expensive problem to solve and one to be avoided. Luckily this situation has rarely occurred at Seattle City Light. Early on we determined that many of our billing systems, which exceeded one million lines of software code, could not accurately handle the year 2000 date.

These are just two examples of how software applications are used to support our most critical business functions. I think you can see how imperative it is for the viability of our business that we fix or remediate these systems. I'm pleased to report that we have now completely remediated all 16 of our mission critical business applications. Furthermore, 14 of these systems have been completely tested and are now in production. Y2K remediation of our major billing system was completed this past spring. It is now in production. Our primary inventory and material management system was remediated and placed in production in early 1998. We are now stepping through the City of Seattle's Y2K certification process for these critical systems. This certification process includes a complete review of our test plans and test results by the City's Y2K project office. It's important to remember that while these applications are very important to our business, none directly impact our ability to generate, transmit, or deliver electricity to our customers. Regardless of this fact, contingency plans are being updated to minimize any impacts that might result from a business application's unavailability.

Power Operations
Along with other utilities in the region, Seattle City Light is an active member of the Western States Coordinating Council (WSCC). The WSCC is the organization that coordinates electric power system reliability in the western United States and Canada. The WSCC and nine other regional councils throughout the continent own the nonprofit corporation commonly known as the North American Electric Reliability Council (NERC). In early May 1998, the U.S. Department of Energy (DOE) asked NERC to assume a leadership role in preparing the electric utilities of the United States for the transition to the Year 2000. DOE's request is part of President Clinton's broad initiative to ensure that infrastructure essential to the nation's security and well being remains operational during critical Y2K transition periods. Seattle City Light has been coordinating its Y2K efforts with other members of the WSCC and NERC.

June 30 was the industry target date NERC established for utilities to have remediation and testing completed for mission critical systems that are used to produce and deliver electricity. These mission critical systems are the foundation of Seattle City Light's electric system. Many of these mission critical power systems can contain date sensitive computerized chips and software that are referred to as embedded systems. These embedded systems may or may not have problems with processing the Year 2000. This would be a significant problem at the utility if our electric system was completely digital and computerized. However, only about 5% of our electric systems' equipment contains embedded systems. For example, of the 5000 protective relays that are used in our system, only 80 contain embedded systems. The vast majority of our field equipment is made up of electro-mechanical devices that pose no Y2K failure risk. However, to assure ourselves that we had identified all mission critical embedded system devices, we hired the TAVA/Beck consulting firm to evaluate the utility's embedded systems inventory. TAVA/Beck combed through representative sites that included powerhouses, major substations, communication facilities, and the System Control Center. Their work helped assure us that we had identified all mission critical embedded systems and that they are Year 2000 compliant.

Our remediation approach has included testing representative samples of date sensitive equipment to determine the existence of Y2K problems and then rolling the dates or replacing devices as needed. As of June 30, all mission critical generation, transmission, and distribution equipment used in the production and delivery of power has been tested, remediated and declared ready for operation in the Year 2000 and beyond. However, we are continuing to test our Energy Management System (EMS). Seattle City Light's EMS is a state-of-the-art system that is used in automated generation, transmission, and power delivery functions. Siemens, the vendor of our EMS has provided us with written assurances that our system is Y2K compliant. Because the EMS is undergoing upgrades, testing will continue through September. We continue to feel confident that the scope of our embedded systems problem is limited, understood, tested and where appropriate, corrected. The bottom line is that we expect business as usual in the Year 2000.

Supplier Readiness

Like most businesses today, Seattle City Light relies upon other companies to provide essential products, material, and services to meet our operational and business needs. Starting in December of last year, we embarked upon an aggressive effort to obtain Y2K compliance information from our vendors and suppliers. Almost 400 vendors have been contacted since that time. We have received an astonishing response rate of almost 90%! This says a lot for Seattle City Light's business partners who have been extremely responsive to our requests for Y2K compliance information. Over half of these businesses are claiming that they are now ready for the Year 2000. Another 25% have indicated that they are not ready now, but will be so by the end of the year. We are in the process of following up on unresponsive suppliers and identifying alternatives, if warranted.

Contingency Planning

The nature of the electric utility industry requires that emergency response procedures be established as an inherent part of its daily operations. Many systems and procedures are already in place to deal with emergencies as they occur. These procedures describe emergency responses to unexpected events such as storm and major outages, total blackout, PCB and oil spills, fire response, dam failure, etc. Guidelines are established for the activation of the City's Emergency Operations Center as well as our utility's Trouble Center, which is always activated in extraordinary conditions.

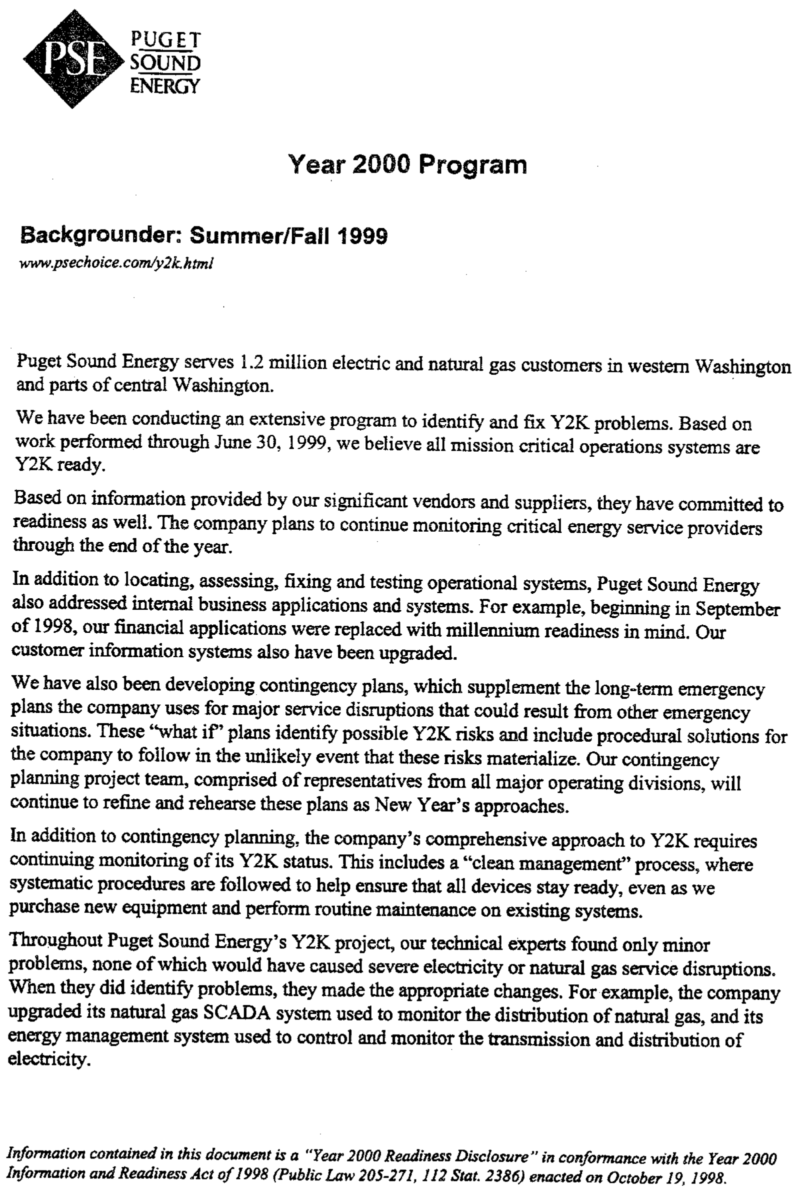
While the millennium rollover presents risk, at least we know when it will happen. Seattle City Light will have special staffing commencing at noon on December 31, 1999 and continuing through noon January 3, 2000. We are determining whether and to what extent special staffing levels should be implemented for other millennium testing dates. Every substation and powerhouse will be staffed during this period. Our Trouble Center will be readied and technical staff will be on alert in case it needs to be activated. Designated engineers will be available on stand-by duty to assist in resolving problems if required. The System Control Center support staff will be on call and available to restore the Energy Management System and its peripherals should they encounter problems. In addition, as active members of the WSCC we have coordinated with other utilities to create a regional Y2K contingency plan, which addresses the interconnectedness of the nation's electric grid. The electric utility industry is accustomed to working together to maintain the reliability of the nation's power grid. For Y2K, Seattle City Light along with other WSCC members and NERC have developed contingency plans that address the needs of our customers, the citizens within the region, and the nation as a whole.

In early April, Seattle City Light successfully participated in a NERC scheduled, continent-wide contingency planning drill. The drill tested the ability to operate the bulk electric system with limited voice and data telecommunications and reduced EMS functionality. This exercise reminded and assured us that we know how to operate our electric system using manual yet highly reliable methods. All of our power plants have the capability of being started even when the plant is completely isolated from the rest of the system. This is known as a "black start." This past spring we performed a "black start" test of one of our main generators located at our Ross Powerhouse. The test was successful as expected. We will be participating in another continent-wide contingency planning test drill scheduled in early September. We are also planning an independent drill to test the procedures for operating the EMS using manual or back-up schemes. This will involve staffing substations and power plants, using alternative methods to determine load calculations and required reserves, and manually controlling generators.

Conclusion

Two weeks ago, Seattle City Light's Year 2000 program was evaluated as part of the City of Seattle's Y2K risk assessment process. The assessment was designed to evaluate the completeness of our Y2K program and to provide current feedback on our efforts to identify and mitigate business risks that may result from Y2K issues. The successful results of this risk assessment reinforced our confidence that Seattle City Light's power will not be interrupted by the transition into the next millennium.

In summary, I would like to thank you for this opportunity to discuss the status of Seattle City Light's Year 2000 readiness and to assure the citizens of this region and our customers that we expect business as usual in the Year 2000. I would also like to take this opportunity to thank Lynn Jacobs and Marty Chakoian of the City of Seattle's Y2K project office who have helped to create and implement a set of much needed citywide Y2K standards and methodologies. Many of these procedures were based on the fine work of the State of Washington. In particular I would like to thank the Washington State Year 2000 Office for leading this state's responsive and timely public outreach efforts. I would also like to thank the many employees throughout Seattle City Light who have directly contributed to the success of the utility's Y2K program in particular, Marlene Flynn and our Y2K project office, the Y2K steering committee, and Superintendent Gary Zarker. Finally, I am grateful for the continued support of our elected officials including Mayor Paul E. Schell and City Council Members Margaret Pageler and Tina Podlodowski.



PUGET SOUND ENERGY

Year 2000 Program

Backgrounder: Summer/Fall 1999

www.psechoice.com/y2k.html

Puget Sound Energy serves 1.2 million electric and natural gas customers in western Washington and parts of central Washington.

We have been conducting an extensive program to identify and fix Y2K problems. Based on work performed through June 30, 1999, we believe all mission critical operations systems are Y2K ready.

Based on information provided by our significant vendors and suppliers, they have committed to readiness as well. The company plans to continue monitoring critical energy service providers through the end of the year.

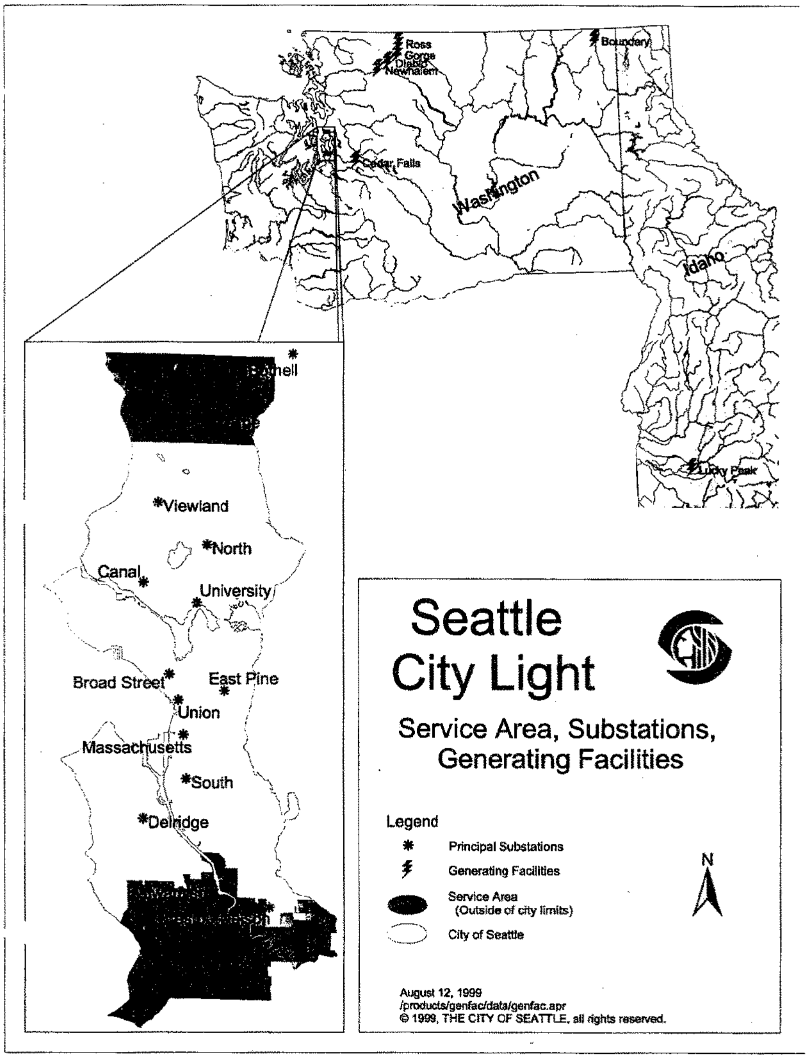
In addition to locating, assessing, fixing and testing operational systems, Puget Sound Energy also addressed internal business applications and systems. For example, beginning in September of 1998, our financial applications were replaced with millennium readiness in mind. Our customer information systems also have been upgraded.

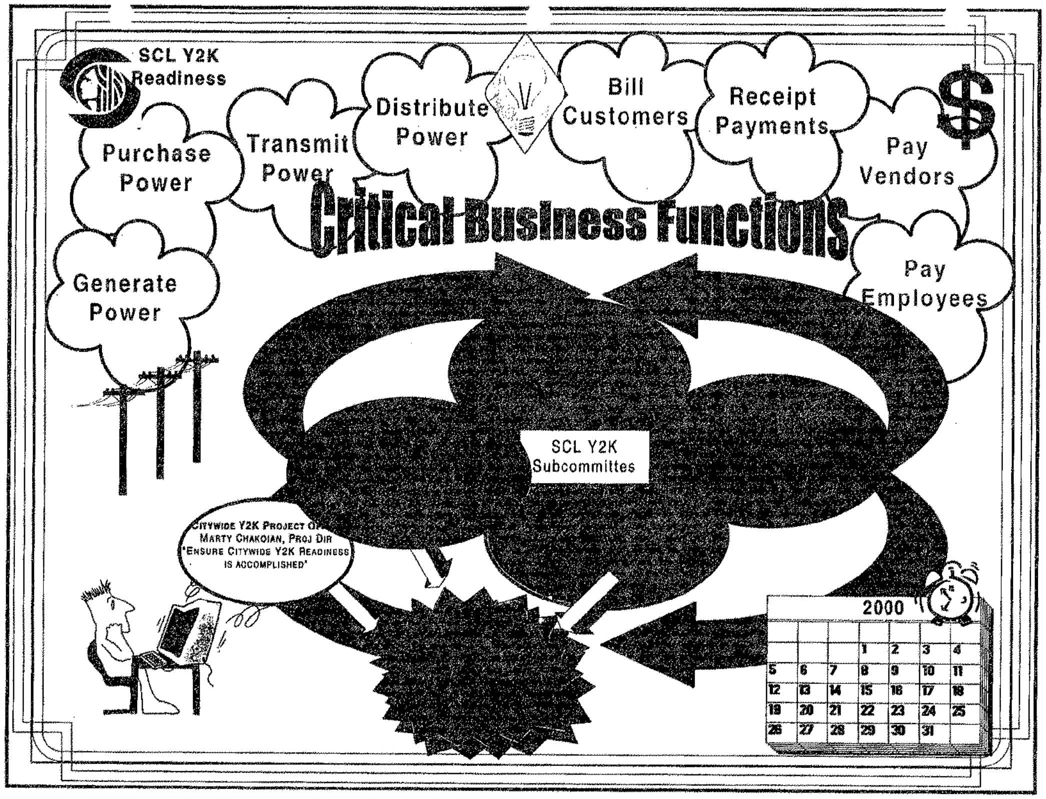
We have also been developing contingency plans, which supplement the long-term emergency plans the company uses for major service disruptions that could result from other emergency situations. These "what if" plans identify possible Y2K risks and include procedural solutions for the company to follow in the unlikely event that these risks materialize. Our contingency planning project team, comprised of representatives from all major operating divisions, will continue to refine and rehearse these plans as New Year's approaches.

In addition to contingency planning, the company's comprehensive approach to Y2K requires continuing monitoring of its Y2K status. This includes a "clean management" process, where systematic procedures are followed to help ensure that all devices stay ready, even as we purchase new equipment and perform routine maintenance on existing systems.

Throughout Puget Sound Energy's Y2K project, our technical experts found only minor problems, none of which would have caused severe electricity or natural gas service disruptions. When they did identify problems, they made the appropriate changes. For example, the company upgraded its natural gas SCADA system used to monitor the distribution of natural gas, and its energy management system used to control and monitor the transmission and distribution of electricity.

Information contained in this document is a "Year 2000 Readiness Disclosure" in conformance with the Year 2000 Information and Readiness Act of 1998 (Public Law 205-271, 112 Stat. 2386) enacted on October 19, 1998.


Ross
Gorge
Diablo
Newhalem
Boundary
Cedar Falls
Washington
Idaho
Lucky Peak
Bothell
Viewland
North
Canal
University
Broad Street
East Pine
Union
Massachusetts
South
Delridge
Seattle
City Light
Service Area, Substations,
Generating Facilities
Legend
Principal Substations
Generating Facilities
Service Area
(Outside of city limits)
City of Seattle
N
August 12, 1999
/products/genfac/data/genfac.apr
© 1999, THE CITY OF SEATTLE, all rights reserved.



SCL Y2K Readiness

Critical Business Functions

Purchase Power

Generate Power

Transmit Power

Distribute Power

Bill Customers

Receipt Payments

Pay Vendors

Pay Employees

SCL Y2K Subcommittes

CITYWIDE Y2K PROJECT OF[illegible]
MARTY CHAKOIAN, PROJ DIR
"ENSURE CITYWIDE Y2K READINESS IS ACCOMPLISHED"

Mr. HORN. Thank you.

The gentleman from Washington, Mr. McDermott.

Mr. MCDERMOTT. I just want to ask this question, because everybody uses this term, an "embedded system," as opposed to what? What's the alternative to an embedded system?

Mr. RITCH. I guess it would be one that could be attached to the side. No.

The term is something that at least I kind of attribute to my technology people, and it's a chip that's embedded, if you will, into a device that you wouldn't think of as data processing.

So I think one of the first examples were elevators and building control equipment. They have chips, clocks, if you will, that regulate when things go on and off, and they get called embedded because the device is embedded in the rest of the equipment.

Mr. MCDERMOTT. As opposed to a computer system sitting at somebody's desk that doesn't have a piece of software in it? Is it software versus chip?

Mr. RITCH. You guys want to take a crack at this one?

Mr. O'ROURKE. An embedded chip is a device, at BPA, for example, that is embedded in our transmission system and sends signals back to our control center that indicate to us the health of that transmission line.

Mr. MCDERMOTT. Those are the problems? The embedded ones? You don't see them, you don't have access to them, they're just out there. Like in my car, where there's embedded systems all through the car.

Mr. O'ROURKE. They certainly are installed by design in our transmission system. And again, that's what gives us control information of the frequency the transmission system is operated at, the quantity of power that's currently being transmitted over the transmission system.

And for additional information, this is Brian Furumasu, our technical expert at Bonneville. I'm sure he can answer the question much more eloquently.

Mr. FURUMASU. Yes, Representative McDermott. I'll give you an example. We use relays to protect our transmission lines. Prior to microprocessors, they were electromechanical devices, so they had no computers at all. Coils, and it was a mechanical device.

So more recently, within the last 10 years, we've had microprocessors now that perform all of those same functions. And those relays are called embedded systems.

Mr. MCDERMOTT. Thank you. Thank you, Mr. Chairman.

Mr. HORN. You're quite welcome. It's a good question. And the Pentagon has millions of them, and that's why they're a little delayed. And as was noted, you have it in your car, you have it in your traffic lights, in most cases you have it in your microwave stove that does your sandwich, and so forth. So they're around, and they are difficult to deal with.

We now have Ms. Hoggarth. Marilyn Hoggarth is the manager of the Washington State public affairs for the General Telephone Co.

Ms. HOGGARTH. Thank you. Well, we, as the other organizations, have already tested our systems for Y2K compliance as of June 30th, and our entire network is ready to go.

We take the opportunity in what we call the maintenance window—after midnight and before 6 a.m.—to repair and test our systems, anyway. And during that timeframe, we've been able to make sure that everything is Y2K compliant.

Regarding our vendors, if a vendor was not able to come up to the bar by the time we needed to be pretested, they simply were not our vendors anymore. We either were able to perform a workaround, have the vendor upgrade the system, or we changed to something else.

A good example of this, although a small and I wouldn't say critical one, but one that's probably easy to visualize, is in Blaine, Washington, an area that we acquired in the ConTel merger several years ago, we had a message manager system, which is a voice-messaging system, that simply was not fixable. That was replaced with the GTE voice mail system. So those kinds of decisions were made down the line on all scales of the switching network.

We, too, will be participating in basically a dry run, shall we say, on September 9th of this year, fully staffing our Emergency Operations Center. That will also be fully staffed on December 31st and into January 1st of next year.

Our Y2K efforts will not end with January 1st. We'll continue operating that office for several weeks after that, and we'll just have to see how it goes. We're confident that the system will work correctly.

Our biggest challenge is to continue to communicate to the public the difference or the demarcation between the public switch network and telephone terminal equipment that sits on someone's desk or in their home.

Any telephone that has date and time sensitivity could be susceptible to Y2K problems. We have set up 800 number hot lines, websites, those types of things, lots of ways for customers to contact us regarding their specific situation. In the case of our major accounts, and this includes the 911 centers that we serve, those will receive individual attention from account managers.

On a broader basis, we're, of course, doing press releases, issuing public information, doing bill inserts—it's questionable how many people read their bill inserts, but we try; it's one way to get ahold of everyone—to let them know that they have responsibility for the telephone equipment that's sitting in their home and business.

Now, some customers are savvy to the fact that there is a difference between the public switch network and many are not. They still think of the telephone system as being one contiguous, end-to-end system, not understanding the whole concept of deregulation there.

The public switched network, being our responsibility, is ready. We do tell people to check with whoever the vendor is for their telephone equipment, and that may not be GTE in many cases. So there is the potential there for a breakdown of the system. If someone has an older PBX, for instance, one of the big switchboards, that type of thing, that we don't maintain, we don't have responsibility for that specifically, and we have been communicating to our customers that they then must check with their vendor for that piece of equipment.

As far as compliance on an international basis, GTE had a role in the Year 2000 Forum in late 1998. We cosponsored the first major Y2K international government and business meeting in London. It was called the Global Year 2000 Summit.

And in connection with the Summit, GTE also hosted a half-day working session dedicated to interoperability testing for other participants. That's for telecommunications networks and systems that will work into the year 2000.

Being an international company, we, of course, have concerns about how everyone will interoperate with telecommunication systems and other companies. I can't speak for their preparedness.

We feel, domestically, that the telephone networks are in good shape, that there should not be a problem there. We certainly expect to have commercial power, but in the instance of not having commercial power, just as we would in any storm situation, we have backup generators in all of our switching offices that have a fuel supply that can keep them going for several days, and, as you'd mentioned before, treat this like it's a bad storm scenario. That is the preparation we're making on that level.

As the manager of our emergency operation center pointed out as he was preparing to staff the center for New Year's Eve, we will have the opportunity to watch the news from across the world and the Nation. And being on the West Coast, should there be anything serious happening on the East Coast, we at least have a few hours to do something about it. Not that we anticipate having to do that, but that is perhaps the luck of the draw for us out here on the West Coast.

We feel we've anticipated everything, but should there be a gremlin out there that we have not anticipated, we're able to watch what happens to the East Coast first.

[The prepared statement of Ms. Hoggarth follows:]

BACKGROUND

GTE
Telephone
Operations

Y2K Testimony From GTE

GTE began formally preparing for Y2K issues in 1995 when we established our Year 2000 Program office in Dallas, Texas to plan and coordinate activities across the country. We currently have up to 1,200 people working on Y2K preparedness nationally and anticipate spending $370 million on the issue.

The Y2K program office has been testing and renovating our software and hardware systems and working with manufacturers and suppliers who provide products and services to GTE. We have also inventoried the date-sensitive products and services we sell to determine their Y2K readiness status. All 13 business units within GTE are preparing our processes across the country.

GTE's Y2K process was among the nation's very first certified under the Information Technology Association of America (ITAA) Year 2000 Program as having met the industry's best practices. GTE is also a member of the Telco Year 2000 Forum, the telephone industry's largest consortium made up of the largest local carriers in the U.S., focused on ensuring that the nation's telephone system performs without major disruption before, during and after January 1, 2000. Forum member companies represent 90 percent of the local access lines operated in the U.S.

Forum members agree that their comprehensive testing supports the fact that call processing will continue without major disruptions as the date changes over on January 1, 2000.

No company in any industry can guarantee a 100 percent flawless entry into the new year. Some isolated service disruptions are possible, but GTE has established definitive contingency plans to remedy any unique disruptions that may arise.

As of June 30 of this year, GTE's telecommunications networks and supporting systems are updated, tested and Y2K ready.

Residential and business customers are receiving information by mail, through bill inserts and via visits from account representatives to help them prepare for Y2K compliance. Selected GTE employees are also making speeches to various community groups on this important topic.

It is important for customers to distinguish between the public switched network and their terminal equipment. Single-line telephone instruments without displays of time or date and/or programmable features probably will not need to be replaced. Unless directly provided by GTE, customers are encouraged to check with the manufacturer of their equipment, to ensure compliance.

New Year's Eve will find crews of employees fully staffing all GTE Emergency Operations Centers across the nation as a precautionary measure. We are confident that GTE customers will be able to ring in the New Year with reliable phone service.

For more information, customers can contact GTE in any of the following ways:

- Via GTE's home page: http://www.gte.com, selecting the "Contact Us" option.
- Send an e-mail message to: online.customer.response@gte.com
- By mail to: GTE Y2K Awareness, HQMO6C13, P.O. Box 152252, Irving, TX. 75015-2252
- By Fax to: 972-507-1272

###

Time on the Move

With glittering balls dropping, revelers cheering and hr blaring, the Year 2000 is sure to be the celebration of... well, of ... century. But when it does arrive, people around the world will be anxiously waiting to see if the computerized business systems that contain internal clocks or perform time-related activities will ring in the new year soundly.

It all stems from the two-digit date shorthand that was used by most early computer programmers, which, for example, replaced 1999 with "99." Everything from large mainframe computers and personal desktop computers to fax machines, modems, printers and everyday software could be affected. But no one knows for sure how extensive the consequences may be.

What we do know is that the so-called "Y2K glitch," "millennium bug" or, simply, "Y2K" isn't just a technical issue. If you've ever been told or had to tell customers that "the computers are down," you know that technology issues quickly translate to very real personal and business consequences.

GTE is among the many international corporations, small businesses, government agencies and individuals working together to greet the new century with confidence.

Easing the Transition

GTE has been aggressively addressing both the technical and business aspects of this challenge with a comprehensive Y2K plan since 1995. Our Y2K efforts are designed to create smooth passage to the Year 2000 – a transition without serious interruption to our network or measurable adverse impact on our customers. To that end, we've dedicated more than $370 million and 1,200 people to the effort, led by an office dedicated solely to Y2K.

Under this plan, we have been assessing possible risks, preparing for the unknown and developing contingency plans, so we will be business-ready before, during and after Jan. 1, 2000. The plan calls for GTE's telecommunications networks and supporting systems to be updated, tested and Y2K-ready by June 1999.

Working Together to Meet the Challenge

GTE's Y2K program tracks the progress of our suppliers' Y2K efforts and works with them to introduce business readiness agreements in new and existing contracts, and we're also sponsoring independent Year 2000 surveys to assess how our suppliers are preparing for the new century. We're working diligently with our E911 customers toward Y2K readiness to have an organized and seamless transition into the Year 2000. Internal business processes, such as order-entry, product design, billing and production, are an integral part of our activities, as well, with departments throughout GTE working together toward the common goal of Y2K readiness.

Into the Future

While we believe we've covered our bases, we can't be too careful. That's why our plan extends into the future, too, with an extensive contingency planning program. The program addresses such topics as maintaining our readiness status up to and beyond Jan. 1, 2000; assigning appropriate staff to various tasks; continuing to work with our customers and business partners; and putting back-up plans in place to help make the transition as seamless as possible.

An Industry Perspective

GTE first disclosed its Year 2000 program information to the Securities and Exchange Commission in 1997 and continues to offer periodic updates to the Commission. In addition, we regularly provide briefings to the Federal Communications Commission, as well as to state regulatory commissions and other state agencies.

In addition, as a charter member of the Telco Year 2000 Forum, GTE is an active participant in voluntary industry efforts related to Y2K. The mission of the Forum is to minimize the risk of network and service failures, to test the functions of date- and time-sensitive operations, and to conduct tests of hardware and software configurations among various networks. Other members include Ameritech, Bell Atlantic, BellSouth, Cincinnati Bell, SBC and U S West.

Leading the Way

In 1996, GTE published the "Criteria for Century Compliar " which became the industry's informal standard for determining [illegible] readiness and continues to be widely used. Further, GTE's Y2K process was among the first (and GTE was the first telecommunications company) certified under the Information Technology Association of America's Year 2000 program.

In addition to GTE's role in the Telco Year 2000 Forum, in late 1998 we co-sponsored the first major Y2K international government/ business meeting – the Global Year 2000 Summit – in London, England. In conjunction with the Summit, GTE hosted a half-day working session dedicated to "interoperability testing" – or how telecommunications networks and systems will work with each other in the Year 2000 and beyond.

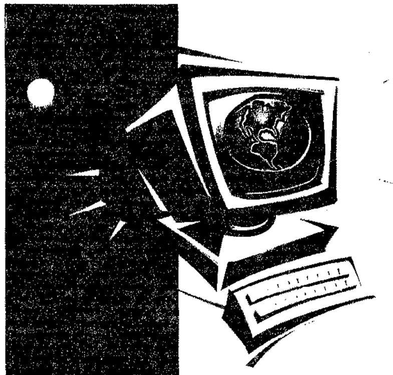
About GTE

With 1998 revenues of more than $25 billion, GTE is one of the world's largest telecommunications companies and a leading provider of integrated telecommunications services. In the United States, GTE provides local service in 28 states and wireless service in 17 states; nationwide long-distance and internetworking services ranging from dial-up Internet access for residential and small-bus' consumers to Web-based applications for Fortune 500 companies; as well as video service in selected markets.

Outside the United States, the company serves nearly 9 million telecommunications customers. GTE is also a leader in government and defense communications systems and equipment, directories and telecommunications-based information services, and aircraft-passenger telecommunications.

GTE PEOPLE MOVING IDEAS℠

The information in this Year 2000 Readiness Disclosure brochure is intended only for general information and increased awareness of Y2K issues. It is current as of March 22, 1999, unless otherwise indicated and is subject to change without notice.



Preparing for the Year 2000

GTE

Y2K Preparedness at GTE

If you have questions regarding how GTE is preparing for Y2K compliance, you can contact the company in one of the following ways:

CALL: 1-800-221-7188

FAX: 1-972-507-1272

INTERNET: online.customer.response@gte.com

Write: GTE
Y2K Awareness
MC: HQM06C13
PO Box 152252
Irving , TX. 75015-2252

GTE Major Accounts should contact their individual account executive.

If your telecommunications equipment (customer premise equipment) is provided by a vendor other than GTE, please contact the vendor directly.

Mr. HORN. Thank you very much.

And next is Dave Hilmoe, the division director of a very important resource that we all need. Maybe we can do without electricity for a while, but you can't do without water. And he's in the Water Quality Supply Division of the Seattle Public Utilities. Mr. Hilmoe.

Mr. HILMOE. Thank you, Mr. Chairman. Marty Chakoian, who was on the previous panel, is actually originally the Seattle Public Utilities Y2K director. He was doing such a good job for us in Y2K preparedness that he was asked to lead the city effort. We hope he's going to come back to us here in another year or so. He's covered a lot of the technology issues and city-wide issues, and so I've got a bit more of an operational focus.

I'm pleased to be here today to tell this committee and our customers that all of our core services—water supply, drainage, wastewater conveyance and solid waste removal—will be ready for the next millennium.

SPU began work on Y2K in 1996. Our Information Technology Division initiated organizational awareness, inventory, assessment and remediation projects. We realize Y2K could have been a serious business continuity issue, but through hard work and intense investigation, we can now say that Y2K is little direct threat to our ability to deliver core services that are essential to our customers.

SPU serves 1.3 million customers, about half directly in the city of Seattle and half through wholesale districts.

Geography and simple technology are the reasons why SPU has low inherent risk from Y2K disruptions. The Seattle water system, although large, is a very simple, redundant, and primarily gravity-fed system. Our main water supplies come from the western slopes of the Cascade Mountains. On average, over 80 percent of the water we supply reaches our direct service customers without any pumping.

We have minimal use of Y2K-vulnerable technology. Our water system monitoring and control consists of mostly older technology, with a heavy reliance on human decisionmaking.

That said, let me give you a few specific examples of what we've done to get ready. We upgraded our current water supply monitoring and control system to a Y2K-compliant version earlier this year. We reviewed all of our supply and treatment-related embedded systems, and replaced those that were not compliant. And we remediated all critical business applications.

We needed to hire an outside contractor to complete and test the one water Y2K-related project that we could not complete on time and with our own staff. We are contacting all of our critical suppliers to reduce risk of service disruption. For example, an adequate stock of disinfection chemicals is going to be on hand, so we have no concerns about transportation or production disruptions.

Our experience with multiple-day power outages at our main treatment plants during the 1993 inaugural day storm, and our experience with other emergencies have supported the creation of detailed, Y2K-specific contingency plans. And the keys to those plans are reliable backup communications, trained staff that are either on duty or on standby during the Y2K boundary period, and the availability of backup equipment.

We are purchasing additional equipment to remove dependency on electricity for water service areas that cannot be gravity fed. We have very high confidence in City Light and Puget Power. This is part of our plan.

Our water supply contingency plans have been tested and refined with two tabletop exercises, and those plans will be integrated now with an additional department-wide testing exercise in September, and a city-wide contingency plan test in October.

The story for drainage and wastewater is similar. Our system is relatively simple. Runoff and sewage primarily flows by gravity from customers to intake points on King County Metro's trunk sewer line and the treatment plant. Where gravity doesn't do the work, we use lift stations.

Critical stations already have backup power. The monitoring system for the 72 lift stations was determined to have a Y2K issue, and is being replaced with a new central system.

Solid waste services have been reviewed for issues related to heavy equipment, contracts for collection and long-haul trucking. Scale house software systems have been upgraded. Readiness of the industrial trash compactors has been assured, and landfill management systems have been addressed. Again, prior experience and existing emergency operations plans have supported development of specific Y2K contingency plans.

We have provided our customers with information on Y2K readiness directly in bill inserts, a webpage, and presentations to community groups—those are going to accelerate here toward the end of the year—and indirectly via reporting to the city of Seattle, State of Washington, and utility associations. And we've been responding to local media requests also in a full and timely fashion.

In short, Seattle Public Utilities is ready for Y2K. We have made our very best efforts to ensure that quality drinking water will continue to flow, and drainage, sewer and solid waste services will all continue to work as usual.

Thank you, again, for the opportunity to testify.

[The prepared statement of Mr. Hilmoe follows:]

City of Seattle
Paul Schell, Mayor

Seattle Public Utilities
Diana Gale, Director

TESTIMONY
Seattle Public Utilities Y2K Readiness
U.S. House of Representatives
Committee on Government Reform
Subcommittee on Government Management, Information, and Technology

By Dave Hilmoe
Director, Water Quality and Supply Member, Y2K Business Continuity Steering Committee
Seattle Public Utilities
Jackson Federal Building
Seattle WA

August 17, 1999

Year 2000 Disclosure

TESTIMONY
Seattle Public Utilities Y2K Readiness

Hello. My name is Dave Hilmoe. I am the Director of Water Quality and Supply for Seattle Public Utilities. I'm pleased to be here today to tell this committee and our customers that all of our core services: water supply, drainage, and wastewater conveyance to the Metro-King County treatment plant, and solid waste removal, as well as customer services, will be ready for the next millennium.

SPU has been working on Y2K issues since 1996. As with most organizations, our Information Technology Division took the lead in those 'early' days, when Y2K was considered merely a very large computer problem. IT initiated organizational awareness, inventory, assessment, and remediation tasks for all computer and embedded systems. We quickly came to realize that Y2K was for SPU a potentially serious business continuity issue – affecting our business operations, monitoring, record-keeping and such. However, extensive work determined that Y2K was significantly less of a threat to our ability to deliver essential municipal services. When it comes to service delivery, our systems are pretty low tech, controlled directly by human operators and aided by gravity. Water flows downhill.

Shortly after the City of Seattle launched its Year 2000 Program Office, SPU created a director level Y2K Business Continuity Steering Committee to complete our Y2K project with the high priority and close coordination it requires. I serve on that steering committee to assure the continuity of water supply and quality. Our Y2K Business Continuity Steering Committee is chaired by our Director of Finance and Administrative Services, Deborah Broughton. Ms. Broughton is our Department Y2K Executive Sponsor reporting directly to Marty Chakoian, Director of the City of Seattle Year 2000 Program Management Office, whom you heard from in the session prior to this, and to Diana Gale, Director of Seattle Public Utilities.

Since the delivery of water is SPU's most critical function, we expect the bulk of your concerns and questions to be with water quality and supply and its Y2K readiness. I am here because I am the executive closest to, and with the deepest knowledge of, the operation of Seattle's water system.

Seattle Public Utilities serves 1.3 million customers, about half directly in the City of Seattle, and half through 26 cities and water districts in the near suburbs. The latter maintain their own delivery and customer billing systems. Foresight, geography, and simple technology are the reasons why SPU has low inherent risk from Y2K disruptions. The Seattle water system although large, is a very simple, redundant, primarily gravity fed system with minimal use of Y2K vulnerable technology. On average, over eighty percent of the water we supply reaches our customers without any pumping.

Our SCADA (Supervisor Control and Data Acquisition) systems are configured with a heavy reliance on human decision making in the operation of water supply, treatment, and distribution systems. That said, let me get specific about some of what we have done to get ready for this challenge.

Examples of what we have done to get ready:

- Our minimal water supply SCADA system, referred to previously, was determined to have a Y2K issue last year. Although not essential to operation of the water system, we upgraded to a Y2K compliant version which was placed in production earlier this year.

- All of our supply and treatment-related embedded systems have been reviewed. Those that were found to have potential issues were replaced and will be rigorously tested following City Program Office standards.

- Water specific business applications have all been remediated, returned to production, and scheduled for a final round of quality assurance Y2K certification testing by the City deadline of September 30. These business applications include our:

  - Work order system
  - Integrated Water Resource Management System
  - Laboratory Management Information System
  - Field disinfection analysis program, and
  - Customer billing system.

We have hired outside contractors to complete and rigorously test the one water Y2K related project we could not complete on time with our own staff. That is the Tolt Dam Monitoring System upgrade, now scheduled to be complete, including certification testing by the end of 3rd quarter.

We are contacting all our critical supply chain partners to make sure these dependencies are managed to remove any risk of service disruption. For example, an adequate stock of disinfection chemicals will be on hand so we'll have no concerns about possible transportation or production disruptions.

Our existing emergency operation plans, our successful experiences with multiple-day power outages at our main treatment plants, and other emergency events such as floods have supported the creation of detailed Y2K- specific contingency plans. The key to these plans are: reliable backup communications, trained staff on duty or on standby during the Y2K boundary period, and availability of backup equipment. We have purchased supplemental equipment including a diesel pump to remove any dependency on electricity for water-service areas that cannot be gravity fed. Our water supply contingency plans have been tested and refined with tabletop exercises in May and July.

Only a couple of weeks ago, we also successfully used portions of these plans during electrical outages caused by a major lightening storm. These plans will be integrated with additional department testing exercises in September and citywide contingency plan testing in October.

Drainage and Wastewater

The story for Drainage and Wastewater is similar. Our system is relatively simple, gravity mostly leads runoff and sewage from customers to intake points on King County Metro's trunk lines leading to their sewage treatment plant at West Point. Where gravity doesn't do the work, we use lift stations. Critical stations already have back up power, and more stations will be so protected before Y2K. The monitoring system that allows operators to confirm operation and react to alarms regarding electricity and pump run times was determined to have Y2K issues and is being replaced with a new central Master Telemetry Unit connected to new Remote Telemetry Units at all 72 lift stations. This system, which has already passed rigorous Y2K bench testing, will be in operation shortly for critical pump stations. All stations are scheduled for connection by mid October.

Solid Waste

Solid waste services were closely reviewed with attention to heavy equipment, contracts for collection and long haul trucking. Scalehouse software systems have been upgraded, the readiness of the industrial trash compactors assured, and landfill management systems addressed.

Again, prior experience and existing emergency operations plans have supported the development of specific Y2K contingency plans for these services as well.

Communications

We have communicated our Y2K readiness with our employees via meetings, publications, and an internal web site. We have provided our customers with information directly in billing inserts, a web page, and presentations to community groups, and indirectly via reporting to the City of Seattle Year 2000 Program Management Office, the State of Washington, and utility associations. We have also responded to local media requests in a full and timely fashion. City review of our Y2K program quality has recognized our very positive, structured, and well staffed approach.

In short, Seattle Public Utilities is ready for Y2K. We are doing everything in our power, to assure that quality drinking water will continue to flow, and drainage, sewer, and solid waste services will all continue to work as usual. Thank you again for this opportunity to present our Y2K readiness status to this committee today.

Mr. HORN. Well, thank you. Water is key.

Brad Cummings, Y2K program manager with the University of Washington Academic Medical Centers. Mr. Cummings.

Mr. CUMMINGS. Chairman Horn, thank you for this opportunity to give you the latest information on our year 2000 preparation activities. Again, I'm Brad Cummings. I represent the University of Washington Academic Medical Centers, which includes the University of Washington Medical Center and Harborview Medical Center.

I'm also accompanied today by Tom Martin, who is the Medical Centers' Director of Information Systems and Chief Information Officer, and Chris Martin, who is Harborview's Administrative Director for Emergency Services.

The objective of the Medical Centers' year 2000 effort is to continue to provide vital services to our patients throughout the Y2K rollover period. As two of the largest hospitals in the Puget Sound area, we recognize the vital role we play in the lives of area citizens, and we have committed significant resources to reduce our exposure to the risk and disruption due to year 2000 issues.

We recognize Y2K as not purely a technical problem, but also a risk mitigation and business issue, with an approach to match.

As referenced earlier, our efforts have been regularly monitored by the State of Washington risk assessment review process, which have helped us to further improve our Y2K procedures.

I've been in this role for 2 years. I am pleased to report on the progress and share information about our overall preparedness.

At this point, 90 percent of our computer systems are now determined to be Y2K compliant, and 100 percent of all systems with the highest priority are Y2K compliant. The remaining computer systems work consists of lower priority items, and we expect to complete that work by September 30th.

Our clinical engineering directors are in the process of completing a major and successful effort to inventory and assess the over 6,000 medical devices on hand at each medical center. Currently, less than 1 percent of those devices are not yet classified as Y2K compliant, and we are upgrading or replacing those devices as soon as they become available from their respective vendors.

Any device that is still not considered Y2K compliant by December will be removed from service at the hospital and alternative procedures will be followed.

Our hospital facilities' systems are all determined to be Y2K compliant at this point. Those include heating, ventilation, air conditioning, security systems, fire alarm systems, and the system to deliver water, steam, and medical gases to where they are needed.

As hospitals, we are also required for our accreditation and licensing to be capable of functioning independently of electrical utility power. So in the unlikely event that power is disrupted, we will have emergency power generators and we will continue to be able to operate vital services at each hospital.

We have recently completed tests at both hospitals in which the regular utility power was shut off. Emergency generator power successfully took over within seconds, allowing the staff to provide vital services and to experience just how the hospital would function under such circumstances.

The Y2K contingency planning we have done has also proved worthwhile in assessing our preparation for other potential emergencies, such as an earthquake.

Although we feel confident in our overall preparedness for Y2K, the reality is that nobody knows for certain what exactly will take place on New Year's Eve, and, as is everyone, we are somewhat dependent on events outside of our direct control.

So we have taken a significant contingency planning effort, using our existing emergency preparedness procedures as the foundation. This includes not only identifying work-arounds in the event that systems or devices are not operating correctly, but we are arranging to have increased staffing on hand over the Y2K rollover period.

Our intent is to have both hospitals' Administrative Command Centers operational on New Year's Eve, and to also closely coordinate with the State and county Emergency Operation Centers to monitor and assess the Y2K situation as it develops.

We are emphasizing to all medical center employees the important relationship between their preparedness at home and their ability to report to work and help maintain full operation of our hospitals.

We are also confident in the area of regional collaboration toward Y2K, particularly among hospitals. Traditionally, regional hospitals have worked together in time of emergency to share needed supplies, take patients if necessary, and perform other steps as required to ensure the continuation of patient care. We have been working closely with the Washington State Hospital Association on Y2K as part of their existing emergency preparation activities. The year 2000 issue lends itself well to collaboration among hospitals, and we see that as another risk mitigation step available to us as necessary.

Finally, it is important to remember that health care services can be provided in a low-tech environment if absolutely necessary. The service may not be as efficient as far as the utilization of hospital staff, and it may complicate billing and collection of payment, but health care is still ultimately provided by skilled professionals who are trained to provide that care even in the absence of high-tech equipment.

The concept of triage is also fundamental, and the medical centers are staffed with professionals who are trained and prepared to allocate potentially scarce hospital resources to the patients who are most in need. In the event that Y2K events disrupt the hospitals, patients will be triaged appropriately to provide the best overall allocation of service the medical centers can provide.

In conclusion, I continue to be impressed with the degree of commitment shown by all levels of the medical centers' personnel, supported by the highest level of administration, for addressing the Y2K issue head-on. And I believe that the University of Washington Academic Medical Center is providing leadership in this area.

If citizens need to be in the hospital over the New Year's period, they can feel fully confident that Harborview and UW Medical Center will, as always, be able to serve whatever vital needs they have. That concludes our remarks.

Mr. HORN. Well, thank you very much, Mr. Cummings.

Let's start with the question I asked the last panel on the management side. If you had to do it over, what have you learned from the management side and when would you have done something else?

Mr. CUMMINGS. I think that the earlier you start Y2K, the better. However, it's important to keep focused on Y2K. I think the contingency planning effort has been vital in this step, looking at how we would operate things if they're not available. And that's been extremely valuable.

I don't think that I would change significantly what we've done as a result of going through this the first time, but I think that, overall, our approach has been good.

Mr. HORN. Mr. Hilmoe.

Mr. HILMOE. Marty Chakoian covered some of that on the last panel. I'd say that starting contingency planning a little bit earlier would have been of some benefit to us for Y2K. We've got an active plan right now, which allowed us to refine that not only for Y2K, but also for other emergencies that we may see here in the Northwest.

Mr. HORN. Ms. Hoggarth.

Ms. HOGGARTH. I would say, from preparation of the network perspective, there wouldn't be anything that we would do differently.

However, you can never have too much public information. As I mentioned before, there will, of course, be people who overreact to the whole Y2K concept, or some that simply choose not to read the information that we've sent them.

Of course, we're prepared for those contingencies, but that would be the one thing that I would suppose you could do more of, but at some point you're at the point of no return.

Mr. HORN. Mr. Ritch.

Mr. RITCH. I think that we would try to get ownership of the problem from the operations people a little bit sooner to get at these embedded systems. It's easy to see where the PCs are. It's a little bit harder to see where some of these other chips might be. So that's one thing.

The other thing, I think, would be to think of this more as an opportunity to talk to your customers and come up with a little better communication strategy for public information.

Mr. HORN. Mr. Walls, anything you'd do differently?

Mr. WALLS. I don't think we would. We started off using a consulting firm that had been through this once or twice before. Along the way, we continued to talk with other utilities up and down the west coast on what worked for them and what didn't.

However, it did seem like it would have been nice to inject somewhat more time in the process. Even though we think we started in time, it's an enormous project. And I don't think we would change much, if anything.

Mr. HORN. Mr. O'Rourke.

Mr. O'ROURKE. I'd echo my colleagues. I don't think we would change our program significantly, but given Bonneville Power Administration's public responsibility, I think we probably could have executed a public information campaign much earlier to give the status of what we have accomplished and get the facts out in the public arena.

Mr. HORN. Since Bonneville is statewide, I'd like to know from each of you the degree, if you have any, of rural customers as opposed to urban. And is there a special problem there in terms of reaching the needs of rural customers as opposed to simply urban, narrow-density, high-density living and this kind of thing?

What about it, Mr. O'Rourke.

Mr. O'ROURKE. Our wholesale customers are comprised of metropolitan areas, rural co-ops. And what we have found is, in the rural environments of the Pacific Northwest, there's far less technology that would compromise distribution of electricity.

Mr. HORN. Mr. Walls? Any rural customers to worry about? Is there a difference in readiness between the rural and the urban customer?

Mr. WALLS. Not at all. The process we use in downtown Bellevue is the same process used in rural Yelm. Same seven-step process of checking every device to ensure that it's ready. There was no difference in the way that we looked at our customers.

Mr. HORN. Mr. Ritch.

Mr. RITCH. All of our customers are in the greater Seattle area.

Mr. HORN. Ms. Hoggarth.

Ms. HOGGARTH. We do have a large number of rural customers. However, our network has been 100 percent digital since September of last year, so there's no difference for the rural customer and the urban one.

Mr. HORN. Mr. Hilmoe.

Mr. HILMOE. We service 26 wholesale districts, primarily in the urban area. Some of them are a bit more rural, some of them are relatively small, and we've got active communication with all of those customers just to make sure that any interdependencies are covered.

Mr. HORN. Mr. Cummings.

Mr. CUMMINGS. Although our patients come from a multistate area, all of our services are provided here in the greater Seattle area.

Mr. HORN. Let me ask my colleague from the State of Washington, Mr. McDermott, if he has some questions.

Mr. MCDERMOTT. Just one sort of personal question after listening to all of this. You say, Ms. Hoggarth, that what sits on my table at home is mine, that you have no responsibility for it. So that means that that AT&T answering machine that I bought 10 years ago is compliant or not compliant? What's going to happen to me?

Ms. HOGGARTH. Well, you need to check with your vendor. And that is our big message. And we do have a GTE Phone Mart at Alderwood.

Mr. MCDERMOTT. But if it simply says to me that on January 2, 1900, Charlie Johnson called me and left the following message, I'm going to get the message, or I'm not going to get the message, or will the phone ring?

Ms. HOGGARTH. Well, that depends. The different types of equipment that are out there are so varied that that is why we're taking the position that you do need to check with whoever provided that to you. If it's an AT&T system, then they, I assume, have an 800 number, as we do. We've also provided some 800 numbers, fax numbers, websites here, where you can contact us with specific questions about your equipment that we will try to answer from our Y2K office in Dallas. If it is, though, something that was provided directly from AT&T, for instance, we would refer you back to them.

Time and date sensitivity, it's so varied from one telephone to the next. If you're simply looking at the basic phone with no caller ID, no date of any kind on it, nothing like that, you don't have to worry. But if you're looking at something that has the built-in features, like the caller ID phones and answering machine, those kinds of things, there is cause for concern, but I couldn't answer for the other vendors.

Mr. MCDERMOTT. So what you're really saying is that everybody should open their bill and read everything in there, including how much they had to pay this month?

Ms. HOGGARTH. At least for the rest of the year.

Mr. MCDERMOTT. At least for the rest of the year. OK. Thank you. Thank you, Mr. Chairman.

Mr. HORN. Here's an interesting one. And I ask all of you this, because it's been a major worry, nationally. Have you tested compliant systems with noncompliant systems? And if so, will the old data corrupt the year 2000 remediated data? What degree has that test gone on?

Mr. CUMMINGS. In some sense, it doesn't make sense to test compliant systems with noncompliant systems. The assumption is they're going to be compliant.

The answer is: it is possible to have corrupt data from noncompliant systems interface with compliant systems and cause problems. What you're doing is looking to isolate yourself from the noncompliant data.

Again, nobody is completely independent. We all interface with different people. That's why it's so important to stay in contact with all of your interface partners to make sure that the data that you are getting is going to be compliant.

Mr. HORN. How about it, Mr. Hilmoe.

Mr. HILMOE. You're asking a civil engineer here, so I need to get our technology person up here to answer that one.

Mr. HORN. As a verification or testing system, did you try noncompliant data? Because that's what we've been told from day one in 1996 when we got into this, is that even if we remediated the code, and that with people abroad, especially in developing nations, that that might pollute our work. And I don't know.

If you've got somebody, great. Let them identify themselves and title of their job.

Mr. DEANE. My name is Thatcher Deane. I'm the Y2K coordinator for Seattle Public Utilities.

Mr. HORN. Just so we've got the name straight—we've got a reporter here that's going to have to translate all this—so spell it out for me.

Mr. DEANE. It's Thatcher, T-H-A-T-C-H-E-R, last name is Deane, D-E-A-N-E.

Mr. HORN. Very good.

Mr. DEANE. And I would actually answer the question this way and say that Y2K is not a computer virus. We're not talking about infection of a compliant system by a noncompliant system. We're talking about the interfaces. And yes, we are looking at all of our interfaces related to our systems.

Mr. HORN. That's very helpful. Ms. Hoggarth.

Ms. HOGGARTH. I'll call on Dennis Smith, one of our local managers.

Mr. HORN. Mr. Dennis Smith. And what is your title with GTE?

Mr. SMITH. I'm the area manager for network operations.

As far as testing compliant and noncompliant systems, I would agree with the gentleman on the end there that we really don't—it is kind of a non-issue, testing compliant with noncompliant.

Mr. HORN. Well, will noncompliant data lead to difficulties with those codes that you've already remediated? Does that cause you to go backward or what?

Mr. SMITH. I suppose that—and I can't accurately answer that question.

Mr. HORN. In other words, you haven't tried to add corrupt data that hasn't been remediated into your system that has been?

Mr. SMITH. We would try to isolate one from the other.

Mr. HORN. OK. Well, that's wonderful if you can know it, but a lot of people are going to connect somehow that don't know it. So I just wondered what type of defenses do you put up in a system like that?

Mr. SMITH. I just don't know that I can accurately answer that question.

Ms. HOGGARTH. I would say from our perspective that once someone tries to hit the public switch network, say, with a telephone that's not compliant, the phone itself isn't going to work, so they're never going to get access going back inbound into the switching network.

As far as our old data on customer records, those types of things, those have all been updated to new systems over the last 4 years. So on an outbound calling basis—we're on a network provisioning basis—we don't have the corrupted data in the network. So to that degree, we're isolated from it.

Mr. HORN. Thank you. Mr. Ritch.

Mr. RITCH. I guess I don't think that I can add much to what Thatcher Deane said about going through all of our interfaces, hand systems, and how they talk to each other to make sure that all of those things are compliant. And in our case, we could make a decision to leave something noncompliant, but that would mean, at least in my view, that we'd stop using it and we would take that system and toss it. So I don't think it's much of an issue, either.

Mr. HORN. Mr. Walls.

Mr. WALLS. During our remediation, for example, on our energy management systems, those systems that manage our transmission and generation system, anything that that connects to, any system that that's integrated with they would test as an overall system.

Literally, Congressman, there are hundreds of tests one will do on each one of these systems to ensure. And like the others, I've looked at the tests, but I don't recall us transporting corrupted data into those systems, because everything we integrate with is compliant or Y2K-ready at this time.

Mr. HORN. Mr. O'Rourke.

Mr. O'ROURKE. Congressman, a key component of our Y2K program was to migrate all of the information that was maintained in our older systems to Y2K-ready systems. So again, to echo some of my colleagues here, it became a nonissue.

Mr. HORN. Mr. Walls, a person in the audience has a question for you, and it says: did you check the embedded chips in each device, or did you just check one of the devices and assume the others with some model number, et cetera, were OK, or did you just ask the vendor?

Mr. WALLS. We did a number of things. Obviously, in a power system where we have 800,000 electric customers with their electronic meters, we did not test all 800,000 meters.

What we did in all areas, whether they're protective relays, metering devices, fault recorders, whatever that device might be, we took a representative example of those devices and then conducted the test.

In some situations, we isolated whole sections of our transmission or generation system and tested a community of devices in an integrated test. So we did not test every device, but we tested enough in each one of the releases and revisions to ensure that we were confident we were Y2K-ready.

Mr. HORN. Mr. Cummings, this is directed to you by a member of the audience, and it's an interesting problem that we face nationwide, and that's prescription drugs. Many are imported. What is being done to stockpile imported medications if our foreign suppliers cannot provide them because of their own Y2K problems? An example is Denmark, which provides one-half of the insulin used by diabetics in the United States.

Mr. CUMMINGS. That's a very good question. We are looking at all of our supplies, including pharmaceuticals, really on an item-by-item basis, to identify the risk associated with each one, and looking at it on a vendor-by-vendor basis as well.

As I mentioned before, traditionally, hospitals have been very collaborative as far as sharing scarce supplies. We are in close contact with the pharmaceutical community, with the vendors and with manufacturers, and we are relying on the information they're providing us.

The reality is that there is definitely some risk, especially as we get outside of the United States. I think I would agree with some of the earlier comments that the United States is better prepared than any other country. Again, we're looking at that as, what are alternatives to different drugs. And that's a challenging question.

Mr. HORN. Thank you. Mr. Willemssen, do you have any sum-up based on this panel? Give the gentleman a live microphone. It's taped with cement to the carpet.

Mr. WILLEMSSEN. One comment. On the question that was raised about data exchanges, and one system being compliant and one system not, let me throw out a different scenario.

Two systems are compliant, according to the organizations. One was compliant due to expanding the date field. The other one was compliant due to a windowing technique that was used. Even though each of those organizations view their systems as compliant, when the data exchange occurs, if it hasn't been adequately tested and addressed for those differing data streams, it won't work properly, and there is the risk of corrupted data.

So going beyond the example that was posed in the question, we even have a problem where one organization says it's compliant and another one does, but unless they've tested that data exchange, you don't know from one end to the other whether it will work as intended.

Mr. HORN. Thank you. That's very helpful.

Well, we're going to move on now. We thank each of you. And we're going to have panel 3: Willie Aikens, the director of companywide process and strategy, the Boeing Co.; Don Jones, director of year 2000 readiness at Microsoft; Joan Enticknap, executive vice president, Seafirst Bank, a Bank of America company; William Jordan, deputy superintendent of public instruction, State of Washington; Rich Bergeon, consultant, NueVue International, Audit 2000.

If you and your staff that might make a written or oral statement would stand up and raise your right hands. And we have three staff members and five witnesses.

[Witnesses sworn.]

Mr. HORN. The clerk will note all of them affirmed.

And we'll start with Mr. Aikens, the director of companywide process and strategy for the Boeing Co.

STATEMENTS OF WILLIE AIKENS, DIRECTOR, COMPANYWIDE PROCESS AND STRATEGY, THE BOEING CO.; DON JONES, DIRECTOR OF YEAR 2000 READINESS, MICROSOFT CORP.; JOAN ENTICKNAP, EXECUTIVE VICE PRESIDENT, SEAFIRST BANK; WILLIAM JORDAN, DEPUTY SUPERINTENDENT OF PUBLIC INSTRUCTION, STATE OF WASHINGTON; AND RICH BERGEON, CONSULTANT, NUEVUE INTERNATIONAL, LLC, AUDIT 2000

Mr. AIKENS. Mr. Chairman, the Boeing Co. is excited that you are holding this conference. We are very, very pleased to share the status of where the Boeing Co. is, and to provide any information to the public that would make this challenge less.

As you'll notice to your right, the Boeing Co. is not an island. This is a world challenge. We have customers in 145 countries, and we operate in 27 States in this country. So my challenge is very easy: all I have to do is keep those 27 States ready for Y2K. And I relish this challenge.

Now, we started, at the Boeing Co., in 1993. We recognized this problem early. Our CEO, Phil Condit, and his staff, were involved.

We report to our board every 2 months. And this has been going on for the last 2½ years. My boss, the CIO, the chief information officer, is responsible for this whole challenge. And I look at this on a daily basis with all of our operating groups.

Now, this is not a new problem, and this is not a separate problem. This is a sustaining, day-to-day situation, and you don't need a brand-new organization to conquer this challenge. And as you will see in some of my charts, this is the way we treated it.

Each operating group must conquer this challenge. It's not something where you can put up a Taj Mahal and say, "All right, you will pull the strings." I just happen to be the program manager, with some program managers in each of our operating groups.

This is the situation. In 1998, we remediated all of our systems. And in 1999—this is what we're all about—they were ready in 1998, and the 1999 challenge was to put them back in production. That's what the problem is here. 98 percent of those are back in production, and the 2 percent are not material; they're being replaced before September 30th.

Now, the key is that we have done, from a business standpoint, scenario testing; i.e., in the Boeing Co., we need to follow the money. So we start with our customers, and we reversed the sequence on processes and systems. And we'll be talking that on my presentation. We're not counting critical computing systems. They are only tools in our process.

And once you look at the scenario testing with the partners and suppliers, then you'll know if you need to have a critical system with a contingency plan. Every system doesn't need a contingency plan. The critical system that might break does.

As you can see, we've followed the normal process of looking at everything, finding it, fixing it, putting it back into production. When you talk Y2K, if you look at the applications, well, we have many applications. They are all back in production. But you don't just concentrate—I need a dial tone—on computers, but I also have to look at things that are outside of my control, and those are the suppliers.

And more importantly—and I won't go through all of these—here is the embedded we've been talking about. These are the product embedded. They're not all equal, but in order to do the Y2K challenge, you need to look at all of these activities, with desktops being the lowest priority. We can always do those. But those are the things that are in my company.

So it boils down to contingency planning. And we talk contingency planning not as an item, but you're looking at rollover and what happens after we cover it.

We profusely took GAO's information and we made sure that we used that guideline. Now we're into making sure that the other people are doing what they should do at our sites.

And as outreach, we've been working at this for the last 4 years. We've been to London, New York, Washington. We've had every meeting with the FAA, and we've had the industries, and also we put the biggest armada of customers, 330, in Seattle.

Now, I could give you more, but you've only given me 5 minutes. For the last 20 seconds, Mr. Chairman and Congresswoman Dunn and counsel, I'd like to take you on a 20-second ride with our chairman, Alan Mulally, who sat in our 737 and looked at whether or not we were ready.

We set the clock back to 11:30 on December 31st. And I'd like for you to put on your safety belts, and let's roll.

[Videotape is played.]

Mr. AIKENS. There are no safety-of-flight issues with our airplane. And I invite you to look at our website, because John Koskinen asked us to put up a website so the small to medium-sized businesses could profit. And if you look at our website, that's exactly what we have done.

[The prepared statement of Mr. Aikens follows:]

Year 2000 Readiness Disclosure

Boeing and the Year 2000 Date Conversion

Testimony to Subcommittee on Government Management, Information, and Technology

Willie C. Aikens, The Boeing Company
August 17, 1999

The Y2K issue exists because many systems, including computer, product-embedded, facilities, and factory floor production equipment systems, utilize a two-digit date field to designate a year. As the century date change occurs, date-sensitive systems may recognize the year 2000 as the year 1900, or not at all. This inability to recognize or properly treat the year 2000 may cause systems to process financial or operations information incorrectly.

State of readiness: The Boeing Company recognized this challenge early, and each operating group started working on the problem in 1993. The Company's Y2K strategy, to make systems "Y2K-ready," includes a common companywide focus on policies, methods and correction tools, and coordination with customers and suppliers. This focus has been on all systems potentially impacted by the Y2K issue, including information technology (IT) systems and non-IT systems, such as product-embedded, facilities and factory floor systems. Each operating group has responsibility for its own conversion, in line with overall guidance and oversight provided by a corporate-level steering committee.

The Company has capitalized on its history of integrating large complex systems, and has an experienced Y2K team and Program Management Office, headed by the Company's chief information officer. Since 1993 the Company has identified, assessed and remediated, if necessary, over 53,000 IT and non-IT systems for Y2K readiness. These systems are now substantially Y2K ready, with the exception of a very few systems that are anticipated to be ready by September 30, 1999.

A companywide, coordinated process to assess supplier readiness began in the second quarter of 1998. This process encompasses four major activities: survey of suppliers, assessment of supplier preparedness, risk mitigation, and contingency planning. The first two activities were completed in 1998 and the remaining activities are scheduled for completion during the third and fourth quarters, respectively, of 1999. The Company is currently developing contingency plans for all high-risk suppliers to mitigate the impact.

Costs to address Y2K issues: The Company's Y2K conversion efforts have not been budgeted and tracked as independent projects, but have occurred in conjunction with normal sustaining activities. The Company estimates that IT Y2K conversion efforts represent the majority of conversion efforts, and have averaged annually approximately $35 million over the last three years, representing on average approximately 10% of the total application-sustaining IT costs during that period. Y2K conversion costs are expected to represent a lower percentage of total application-sustaining IT costs in 1999. In addition to these sustaining costs, the discretely identifiable IT costs associated with Y2K conversion activities are expected to total $16 million. The Company does not expect a reduction in sustaining costs when Y2K conversion activities are completed because normal sustaining activities will be ongoing. Reprioritizing sustaining activities to support Y2K has not had, and is not expected to have, an adverse impact on operations.

Risks associated with Y2K issues: Due to the Company's early recognition and start on resolving the Y2K issue, the Company believes there is low risk of any internal critical system, product-embedded system, or other critical Company asset not being Y2K-ready by the end of 1999. The Company continues to assess its risk exposure due to external factors and suppliers, including suppliers outside the United States. Additionally, the Company is working with its customers and suppliers, conducting test scenarios to assess Y2K readiness. Although the Company has no reason to conclude that any specific supplier represents a significant risk, the most reasonably likely worst-case Y2K scenario would entail production disruption due to inability of suppliers to deliver critical parts.

The Company's contingency planning has been divided into two phases: Phase I - Develop a Year 2000 Corporate Business Continuity and Contingency Plan; and Phase II - Implement Business Continuity and Contingency Plan through the Site Transition Plan. Phase I is complete. The Company has developed a risk assessment-based Year 2000 Business Continuity and Contingency Plan consistent with the Company's computing disaster preparedness goal, which is to "reduce vulnerability and enhance risk management." Where appropriate, this plan leverages existing Company system and supplier contingency and disaster recovery planning. This contingency planning incorporates information from leading information technology organizations in the industry and government, including the U.S. General Accounting Office (GAO) guideline, "Year 2000 Computing Crisis: Business Continuity and Contingency Planning," dated August 1998. The plan provides a structured approach to assist operating groups with business continuity and contingency planning. Phase II – Implement Business Continuity and Contingency Plan through the Site Transition Plan – is ongoing. A Site Year 2000 Transition Plan template has been developed which outlines the specific staffing and contingency plans for before, during and after the year 2000 rollover, and further describes the major elements required to complete the plan. Each operating group is developing and implementing a Site Year 2000 Transition Plan. Each group's progress is reported to the Year 2000 Program Management Office on a monthly basis. The Company continues to work closely with local, state, and federal emergency management organizations to ensure coordinated plans are in place should infrastructure problems occur in the year 2000.

Forward Looking Information is Subject to Risk and Uncertainty

Certain statements in this testimony contain "forward-looking" information that involves risk and uncertainty, including discussions of plans for addressing the Year 2000 challenge, timetables for accomplishing such plans, and the costs of implementing such plans. Actual future results and trends may differ materially depending on a variety of factors, including the Company's successful execution of internal performance plans including technical solutions to the Year 2000 problem, and performance issues with suppliers, subcontractors and customers. Additional information regarding these factors is contained in the Company's annual Report on Form 10-K for the year ended 1998 and Form 10-Q for the quarterly period ended June 30, 1999.

Mr. HORN. That's very helpful. I agree with the Minister of China, that when Mr. Shuster, chairman of our Transportation Committee on which I serve, went over there, and he said, "No Boeing, no going."

Now, why some of their cousins are getting an Airbus, I'm wound up on that subject this week. So we'll see what happens.

Anyhow, let us go on now to Mr. Jones, who is the director of the year 2000 readiness at Microsoft. Glad to have you here.

Mr. JONES. Mr. Chairman, on behalf of Microsoft, Bill Gates, and Steve Ballmer, thank you for inviting us to testify. In addition, we'd like to thank you for your passage and support of the Information Readiness and Disclosure Act, as well as the recently passed Y2K Act.

My remarks today center around four key areas. The first is Y2K and the personal computer, followed by Microsoft's efforts in three areas, internal readiness, product readiness, and customer readiness.

As the year 2000 relates to the personal computer, there is some good news. The PC was always designed to support four-digit dates. There is no two-digit date usage within the PC in Microsoft software.

There's been a lot of discussion today about compliance definitions. What we've determined is the compliance definitions globally have many different meanings, and they vary within the United States, even by agency. This makes it very hard for an organization to declare compliance. We've applied a set of compliance criteria to our products, and I'll discuss that later. What we're seeing as far as customers and government and where they're at now with the year 2000 programs: most have moved on from requesting product information from Microsoft to really focusing on contingency planning with Microsoft as a vendor. We'll be there for them should they have any issues come January 1, 2000.

We've seen inadequate work to date in contingency planning, both within the government sector as well as in small and medium businesses, and finally enterprises.

One concern that we do have is some economic data that's beginning to become apparent, and that's that about three-tenths of 1 percent of the GDP will move into 1999 from the year 2000. That means companies are going to stockpile at least a percentage of their raw materials preparing for the year 2000. This could cause a downturn in earnings across corporate America in the first quarter of the calendar year 2000.

Microsoft's year 2000 program has three facets: customer preparedness, product readiness, and internal preparedness.

On the customer preparedness front, there was discussion earlier today about quelling the masses as it relates to hysteria with respect to Y2K. We've launched a consumer campaign which will contact 60 million users of Microsoft products across the globe. According to the Postal Service, this could be the largest mailing, ever, beyond tax forms.

We've developed a program which encompasses what the year 2000 challenge is and made it very simple for our end users, our customers, essentially being hardware, software and data. With respect to hardware, contact your PC manufacturer; with software, we've got a great website, as do the other software manufacturers; and finally, data, and that's converting your two-digit date data to four-digit date data.

Of note in the customer preparedness area, all Microsoft information, resources and tools are free as it relates to the year 2000, as is our customer support or dial-in lines. To quantify that for the committee, we expect to ship approximately 18 million resource CDs globally, which equates to about the same number of CDs we shipped of Windows '95.

Our internal effort consists of about 300 or so people in development, and about 3,000 overall in supporting our customers. On the product preparedness front, we've tested 3,200 products to date. Of those, 98 percent are compliant. Of note, the panel members who presented to you earlier today have all been testing Microsoft products as well. We feel this is the largest industry testing effort, ever. And to date, we've had exactly one customer-reported bug as it relates to Microsoft products.

On our website utilization, we have three: a consumer website designed for the average home user or small business; an IT pro website designed for enterprise customers and large businesses; and finally, a developer website, designed for people using Microsoft development tools to build applications.

We've experienced approximately 10 million unique users to these three websites in the last year. We've delivered 45 million page views of information.

Of note, we're seeing dramatic increases in the last three months of small businesses and consumers returning to us for information resources. That increase has been on the order of about 107 percent per month, month over month, for the last three months. We think this is excellent news, and it goes to demonstrate the great work being done by the SDA and the industry in rallying consumer awareness for the year 2000.

As it relates to internal preparedness, our definition of being prepared internally is: no impact on operations. We have the ability to develop and distribute patches and resolve customer issues with or without power. We have battery backup and generator backup to our product support services locations globally.

One thing I do want to close with—I understand I've got 30 seconds left or so—one issue that keeps us awake at night is the concept of malicious viruses being launched on or about the year 2000. To date, we've had seven that have been instigated that looked like they were launched from Microsoft, which, in fact, weren't. We're working with the Federal Bureau of Investigation to find the perpetrators of those and to bring them to justice.

But clearly, we think the year 2000 is an opportunity for hackers to develop viruses and launch them either at the turn of the millennium or in the new millennium. And that concludes my comments. Thank you.

Mr. HORN. Thank you very much. That's helpful. And I'm glad to say the perpetrators have been nailed.

Joan Enticknap is the executive vice president, Seafirst Bank, and you're now a Bank of America company. Welcome. It's a great bank.

Ms. ENTICKNAP. Thank you. Thank you, Chairman Horn and Congresswoman Dunn, for this opportunity to testify on the important issue of year 2000 preparedness. My name is Joan Enticknap, and I am the manager of Commercial Banking for Washington and Idaho for Seafirst Bank, a Bank of America company. I am also responsible for year 2000 preparedness for the Northwest region.

Seafirst has been serving customers in Washington State for 129 years, and is Washington State's largest commercial bank.

Bank of America, with $614 billion in assets, is the largest bank in the United States. And the company serves more than 30 million households and over 2 million businesses, offering customers the largest and most convenient delivery network.

I am pleased to be here today and to share with you the plans our company has put in place to make the year 2000 date change a non-event for our customers.

The banking industry is squarely in the center of attention because of its critical role in our national infrastructure and the role it plays in how our communities perceive and ultimately react to the date change.

I am proud to say that the financial services industry has been recognized as a leader in year 2000 preparedness. As one example, the GartnerGroup, a technology research and consulting group, has stated that the financial services industry leads all other industries in preparedness.

Our various regulators are closely monitoring the banking industry's relative strength and readiness in its preparations. Our industry is being monitored by the President's Council on Year 2000 Conversion, and our industry's state of readiness is a matter of public record and can be found at any number of regulatory websites.

As a federally chartered and federally insured bank, we are held to rigorous oversight by the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Board of Governors of the Federal Reserve.

At Bank of America, our goal is to thoroughly prepare our company and its subsidiaries for year 2000, and make the date change a non-event for our customers. As part of the Bank of America organization, Seafirst Bank has been an active participant in these efforts.

Through its predecessor organizations, NationsBank Corp. and BankAmerica Corporation, Bank of America began addressing the year 2000 in 1995. Through the second quarter of 1999, we have spent approximately $477 million on year 2000 preparations, and more than 3,000 people have worked on the project.

Our approach included four phases. The first phase, analysis, required us to inventory our software and systems, including over 4,400 systems and projects that needed analysis and possible modification.

The second phase, remediation, involved replacing, modifying, or retiring appropriate components as identified during the analysis phase. We were substantially complete at the end of 1998 with that process.

The third phase is testing, which assesses whether our systems identify and process dates accurately. This involves testing the links between our internal systems as well as testing interconnections between our systems and systems outside the bank. By itself, testing has made up over half of our year 2000 efforts.

The fourth phase is compliance. In the compliance phase, we internally certify that systems, projects and infrastructure are ready for year 2000, and we implement processes to ensure that these systems, projects and infrastructure will continue to identify and process dates accurately through the year 2000 and thereafter.

We have successfully met our year 2000 deadline of June 30, 1999, for testing key processes and technology, and have met all Federal regulatory requirements. With this major achievement, we are ready for January 1, 2000.

Now that we are ready for 2000, we are devoting considerable effort to maintaining that status. We are also devoting considerable effort to addressing and monitoring the status of our 13,000 vendors.

Another important part of our process, which you've heard a lot about today, is business continuity planning. We have built on our experience of continuity planning, and we've dealt with continuity plans routinely in a company of this size. We're refining and testing our existing continuity plans to ensure that we will continue to serve customers in case of any incidents related to the date change.

Beyond that, we think communication will play a key role in how our customers and associates and our communities respond to change. Therefore, we're regularly communicating with our consumers, corporate and commercial customers, and that includes suggested steps to our consumers on how they can prepare for year 2000.

As I stated earlier, our goal is to make the date change a nonevent for our customers. Just as we do today, we will maintain the safety, security, and accuracy of customer accounts and account records through the millennium and beyond.

We are aware, however, that a number of organizations and individuals are recommending that consumers take some or all of their money out of the bank. We encourage customers to seriously consider the security implications of doing this.

In conclusion, I want to summarize our industry's and my company's state of readiness for year 2000. Our industry is a leader in year 2000 preparedness, and Bank of America has been addressing the date change issue since 1995, and we are ready for the year 2000.

Thank you for the opportunity to update the committee on our industry and our company's preparedness.

[The prepared statement of Ms. Enticknap follows:]

TESTIMONY OF

JOAN ENTICKNAP
SEAFIRST BANK
(a Bank of America Company)

before the

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

of the

TASK FORCE ON THE YEAR 2000
U.S. HOUSE OF REPRESENTATIVES

August 17, 1999

Thank you, Chairman Horn, Congressman McDermott, and Congresswoman Dunn for this opportunity to testify on the important issue of Year 2000 preparedness.

My name is Joan Enticknap and I am the manager of Commercial Banking for Washington and Idaho for Seafirst Bank, a Bank of America company. I am also responsible for Year 2000 preparatory work for the Northwest Region. During my twenty-one years with Seafirst and Bank of America, I have held a number of positions, including Chief Financial Officer, Retail Delivery Systems Manager and Manager of Technology Strategy.

Seafirst has been serving customers in Washington State for 129 years, and is Washington State's largest commercial bank.

Bank of America, with $614 billion in assets, is the largest bank in the United States. The company serves more than 30 million households and 2 million businesses across the country, offering customers the largest and most convenient delivery network from offices and ATMs to telephone and internet access. It also provides comprehensive international corporate financial services for clients doing business around the world. The company creates financial relationships featuring a full array of financial services, from traditional banking products to investments and capital raising within the securities markets. Bank of America stock (BAC) is listed on the New York, Pacific and London stock exchange.

I am pleased to be here today and share with you the plans our company has put in place to make the year 2000 date change a non-event for our customers.

My testimony will be in three parts. I will address the general state of readiness of the nation's banking industry. Next, I will speak specifically to what my company is doing to prepare for the date change. And, last, I will provide what we think are prudent steps for consumers to take in considering the impact of the year 2000.

The banking industry, together with utilities and telecommunications companies, is squarely at the center of attention because of its critical role in our national infrastructure and the role it plays in how our communities perceive, and ultimately react to, the date change.

The financial services industry has been recognized as a leader in year 2000 preparedness. As an industry accustomed to change, we recognized the importance of addressing this issue early on, and committed significant resources to prepare our systems.

Industry experts have consistently rated banks number one in year 2000 preparedness. The Gartner Group, a technology research and consulting group, has stated that the financial services industry leads all other industries in preparedness. Research from the Tower Group, a highly respected industry consuiting group, cited that the banking industry has invested more than $8 billion dollars to address Year 2000.

Our various regulators are closely monitoring the banking industry's relative strength and readiness in its year 2000 preparations.

Our industry's efforts are also being monitored by the President's Council on Year 2000 Conversion, the group that serves as a liaison between the federal government and regulatory agencies.

In addition, information about our industry's state of readiness is a matter of public record and can be found at any number of regulatory agency web sites.

As a federally chartered and federally insured bank, we are held to rigorous oversight by the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation and the Board of Governors of the Federal Reserve, all of which adhere to the Y2K guidelines published by the Federal Financial Institutions Examination Council.

As a publicly traded company, we are required to regularly report our Y2K status in 10Q and 10K filings made to the Securities and Exchange Commission.

At Bank of America, our goal is to thoroughly prepare our company and its subsidiaries for Year 2000 and to make the date change a non-event for our customers. As part of the Bank of America organization, Seafirst Bank has been an active participant in these efforts.

We recognized early on that Year 2000 is as much a business issue as it is a technical issue, and we have approached it from that standpoint.

Our efforts were to consider all aspects of our business from Seattle to Singapore, from mainframe computers to personal computers, and the vendors and business partners that work with us every day.

Through its predecessor organizations, NationsBank Corporation and BankAmerica Corporation, Bank of America began addressing the year 2000 in 1995. Through second quarter 1999, we have spent approximately $477 million on year 2000 preparations, and more than 3,000 people have worked on the project.

Our approach includes four phases.

The first phase, analysis, required us to inventory our hardware, systems and applications as well as our infrastructure, which comprises the non-computer equipment, buildings and services that contain imbedded microchips or other forms of microprocessors. We identified approximately 4,400 systems and projects that needed analysis and possible modification to be ready for Year 2000.

The second phase, remediation, involved replacing, modifying, or retiring appropriate components as identified during the analysis phase. With respect to our mission-critical systems – those vital to serving customers – the remediation phase was substantially complete at the end of 1998.

The third phase is testing, which assesses whether our systems identify and process dates accurately. This involves testing the links between our internal systems as well as testing the interconnection between our systems and systems outside the bank, like those maintained by agencies and service providers. By itself, testing has made up more than half of our year 2000 efforts.

The fourth phase is compliance. In the compliance phase, we internally certify the systems, projects and infrastructure that are ready for Year 2000, and we implement processes to enable these systems, projects and infrastructure to continue to identify and process dates accurately through the year 2000 and thereafter.

We have successfully met our June 30, 1999, goal for testing key processes and technology, including applications, hardware, software, and networking equipment, and have met federal regulatory requirements. With this major achievement, we are ready for January 1, 2000.

Now that we are ready for Year 2000, we are devoting considerable effort to maintaining that status. We continue to test and retest vital systems, both internally and with outside parties, and we will be carefully controlling systems changes, especially during the last quarter of 1999.

We have also devoted considerable effort to assessing and monitoring the Year 2000 status of our more than 13,000 vendors.

Another important part of our effort is business continuity planning, which will allow us to be prepared for Year 2000 issues that could affect our ability to serve our customers.

With respect to continuity planning, we have built on our experience in preparing plans to address issues that are dealt with routinely at a company our size – power outages, weather or other natural events, systems or vendor problems, or other matters. We are refining and testing our existing business continuity plans to enable Bank of America to continue serving customers in case of incidents related to the date change.

As I mentioned earlier, it is important to realize that this is not only an issue with hardware and software, it is a business issue, and we have approached it that way. We have looked at all the roles we play as an institution – from lender to investment manager, from trustee to tenant – and have considered the potential issues the date change could raise in each case.

Beyond all this, we think communication will play a key role in how our customers, our associates and our communities respond to this issue.

We have established a number of communication efforts. We communicate regularly with our corporate and commercial customers. We have information available for our retail customers on our web site and we have launched a proactive customer communication program.

In May of this year, Year 2000 brochures were added to display racks in banking centers, and in June, a toll-free Year 2000 Information Line was introduced. That number is 1-888-960-1111. Customers will periodically receive information in their checking account statements and through other channels. Our web site, www.bankofamerica.com, enables customers to have direct access to Year 2000 information.

As stated earlier, our goal is to make the date change a non-event for our customers. Just as we do today, we will maintain the safety, security and accuracy of customer accounts and account records through the millennium and beyond.

Finally, Mr. Chairman, I would like to provide some context around consumer concerns and many of the issues being raised in the media. We think there are some very basic, prudent steps consumers can take to help prepare for the year 2000 date change.

We recommend consumers review and maintain statements and records of their financial transactions, as they always should.

We encourage consumers to contact businesses and services they depend on to learn about their Y2K preparedness plans.

We also recommend that consumers determine if their personal software and PC are ready for the date change.

In general, we encourage consumers to stay informed about the issue, balance what they learn through the media, and take reasonable steps when considering how Year 2000 will impact them.

We are aware that a number of organizations and individuals are recommending that consumers take some or all of their money out of the bank. We strongly encourage customers to consider the security implications of doing this.

While we must all take this event seriously and make prudent and reasonable judgments about its impact on us as consumers, we also must avoid the outcome described by the comic strip character Pogo when he said – quote:

"We have met the enemy and he is us."

In conclusion, I want to summarize our industry's and my company's state of readiness for the year 2000. Our industry is a leader in Year 2000 preparedness. Bank of America has been addressing the date change issue since 1995 and we are ready for the year 2000. We will maintain the safety and security of our customers' accounts through the date change and into the 21st century.

Once again, Mr. Chairman, thank you for the opportunity to update the Subcommittee on Government Management, Information, and Technology on our industry's and our company's state of preparedness for year 2000. We will remain diligently focused on this issue, and I will be pleased to keep you informed of our approach going forward.

Mr. HORN. Well, thank you very much. That's most helpful.

Mr. Jordan is the deputy superintendent of public instruction for the State of Washington.

Mr. JORDAN. Thank you, Chairman Horn, Representative Dunn. I'm Bill Jordan, deputy superintendent of public instruction for the State of Washington. The K–12 education system for Washington's 1 million K–12 students includes 296 school districts and 2,071 school sites.

I'm happy to have this opportunity to discuss Y2K concerns with you, because this is an important opportunity for Federal, State, and local governments to work together in ensuring Y2K compliance and assisting community efforts to be prepared for any related problems that may arise.

Most of the Y2K work at the State level in the educational organization has taken the form of checking internal electronic data systems and mechanical support systems to guard against potential blowouts and loss of important electronic data, basic heat and light systems, and vendor services.

As an agency, the Office of Superintendent of Public Instruction has contacted the nine educational service districts, ESDs, throughout this State to verify activities of local districts and schools. Our educational service districts have provided workshops, information, and, in some instances, considerable technical assistance to help school districts and schools prepare for avoiding potential Y2K problems.

Generally, midsize and larger districts have worked on checking electronic equipment and developing Y2K plans. At educational Service District 112 at Vancouver, they have been very active in helping the 30 districts in their region qualify for risk management insurance. They've developed a Y2K planning manual and helped districts make plans for a variety of contingencies and scenarios that could result from Y2K problems.

Other ESDs and districts——

Mr. HORN. Excuse me. Do you have a copy of that document?

Mr. JORDAN. I do.

Mr. HORN. Great. I'd like it inserted in the record at this point without objection. Thank you.

[The information referred to follows:]

Prepared Statement for House Subcommittee on
Government Management, Information and Technology
Committee on Government Reform

"Is Seattle prepared for Y2K"

University of Washington Academic Medical Centers

August 17, 1999

Chairman Horn and members of the Subcommittee, the University of Washington Academic Medical Centers (UW Medical Center and Harborview Medical Center) appreciate this opportunity to provide you with the latest information on our Year 2000 Preparedness activities. I am Brad Cummings, the Year 2000 Program Manager for the Medical Centers. I am accompanied today by Tom Martin, the Medical Centers' Director of Information Systems and Chief Information Officer, and Chris Martin [no relation], Harborview's Administrative Director for Emergency Services.

The objective of the Medical Centers' Year 2000 effort is to continue to provide vital services to our patients throughout the Y2K rollover period. As two of the largest hospitals in the Puget Sound area, we recognize the vital role we play in the lives of area citizens, and we have committed significant resources to reduce our exposure to the risk of disruption due to the Year 2000 issue. Our commitment is illustrated by the composition of the Y2K Advisory Committee, which is chaired by the Executive Director of the UW Medical Center, and is comprised of key administrators from both Medical Centers. We recognize Y2K as not purely a technical problem, but also a risk mitigation and business issue, with an approach to match. Our efforts have been regularly monitored by the State of Washington's Risk Assessment Reviews, which have helped us further improve our Y2K procedures.

Two years after assuming this role, I am pleased to report on the progress and share information about the Medical Centers' overall Y2K preparedness. Ninety percent of our computer systems are now determined to be Y2K-compliant, as defined by the State's Dept. of Information Services, and 100% of all systems with the highest priority are Y2K-compliant. The remaining computer systems work consists of lower priority items, and we expect to complete that work by September 30.

Our Clinical Engineering Directors are in the process of completing a major and successful effort to inventory and assess the over 6000 medical devices on hand at each Medical Center. Currently, less than 1% of those devices are not yet classified as Y2K-compliant, and we are upgrading or replacing those devices as soon as they become available from their respective vendors. Any device that is still not considered Y2K-compliant by December will be removed from service at the hospital, and alternative procedures will be followed.

Our hospitals' facilities systems are all determined to be Y2K-compliant at this point. This includes heating, ventilation and air conditioning (HVAC) systems, security systems, fire alarm systems, elevators, and the systems that deliver water, steam, and medical gasses to where they are needed. As hospitals, we are also required for our accreditation and licensing to be capable of functioning independently of electrical utility power; in the event that power is disrupted, we will have emergency power generators and we will continue to be able to operate vital services at each hospital. We have recently completed tests at both hospitals in which the regular utility power was shut off; emergency generator power successfully took over within seconds, allowing the staff to provide vital services and to experience just how the hospital would function under such circumstances. The Y2K contingency planning we have done has also proven worthwhile in assessing our preparation for other potential emergencies such as an earthquake.

Although we feel confident in our overall preparedness for Y2K, the reality is that nobody knows for certain what exactly will take place on New Year's Eve, and, as is everyone, we are somewhat dependent on events outside of our direct control. Hence, we have undertaken a significant contingency planning effort using our existing emergency preparedness procedures as the foundation. This includes not only identifying workarounds in the event that systems or devices are not operating correctly, but we are arranging to have increased staffing on hand over the Y2K-rollover period. Our intent is to have both hospitals' Administrative Command Centers operational on New Year's Eve, and to also closely coordinate with the State and County Emergency Operations Centers to monitor and assess the Y2K situation as it develops. We are emphasizing to all Medical Center employees the important relationship between their preparedness at home and their ability to report to work and help maintain full operation of our hospitals.

We also feel confident in the area's regional collaboration toward Y2K, particularly among hospitals. Traditionally, regional hospitals have worked together in times of emergency to share needed supplies, take patients if necessary, and perform other steps as required to ensure the continuation of patient care. We have been working closely with the Washington State Hospital Association (WSHA) on Y2K as part of their existing emergency preparation activities. The Year 2000 issue lends itself well to collaboration among hospitals, and we see that as another risk mitigation step available to us if necessary.

Finally, it is important to remember that health-care services can be provided in a "low-tech" environment if absolutely necessary. The service may not be as efficient in terms of utilizing hospital staff, and it may complicate billing and collection of payment, but health care is still ultimately provided by skilled professionals who are trained to provide that care even in the absence of high-tech equipment. The concept of triage is also fundamental, and the Medical Centers are staffed with professionals who are prepared to allocate potentially scarce hospital resources to the patients who are most in need. In the event that Y2K events disrupt the hospital, patients will be triaged appropriately to provide the best overall allocation of the service that the Medical Centers can provide.

In conclusion, I continue to be impressed with the degree of commitment shown by all levels of the Medical Centers' personnel, supported by the highest level of the administration, toward addressing the Y2K issues head on; and I believe that the UW Academic Medical Center is providing leadership in this area. If citizens need to be in the hospital over the New Year's period, they can feel fully confident that Harborview and the UW Medical Center will, as always, be able to serve whatever vital needs that they have.

I thank you again for the opportunity to address the Subcommittee, and we would be pleased to answer any questions that you may have.

Mr. JORDAN. Other service districts have worked in similar ways. Potential problem areas are likely to be in smaller districts, with limited numbers of staff and resources to deal with in-depth planning and preparation. These districts and communities need expertise and resources. Community planning has often taken the form of planning for a 3-day event. We now realize that there is potential for a longer period of disruption and the need for a larger coordinated effort to move toward full community preparedness.

Controlled tests of community systems reveal two things. First, there is a broad interdependence of community electronic systems. A water system may be compliant and functioning, but its interactions with other systems may place a strain on both systems and lead to failure and resulting problems.

Tests need to involve the range of community systems—electronic systems, utilities, transportation, distribution systems, and all type of electronic tools and appliances.

Critical needs, such as heat, water, food distribution, transportation, communications, health care and other interconnected services could be affected.

Second, many have focused on the prevention of problems but less on contingency plans and broader community preparedness. All of us hope that the efforts taken to date will be sufficient to avert any disruption. Given the pervasiveness of automated electronic systems and the widespread use of embedded chips, it's difficult to guarantee that all systems will function. It's imperative that communities are prepared to meet any problems that may arise.

Preparation for Y2K should be no different from any other form of emergency. Community preparedness for any disruption or emergency is the right thing to do. Schools frequently play an important role in providing shelter, food and support for other needed community services.

I'm recommending that Federal, State and local governments and community agencies join together actively and visibly in a careful evaluation and promotion of community preparedness. This preparedness must extend beyond the checking of electronic systems and include preparedness for related Y2K disruptions as well as other possible disasters or emergencies that would call on community schools as a resource.

We recommend the following: citizen education programs that provide guidance to citizens about the potential problems that might be experienced; local contingency planning and preparedness efforts that can give citizens a sense of confidence that they will not be left alone to cope with problems or emergencies; controlled community preparedness tests that build coordinated community interagency capacity to deal with emergencies—local emergency management offices can provide valuable leadership in this area; the coordination of Federal, State and local actions can provide early responses to possible needs for water, food supplies, fuel, shelter and emergency services.

I want to thank you again for this opportunity to talk about Y2K preparedness in our schools in Washington State.

[The prepared statement of Mr. Jordan follows:]

Y2K Preparedness
Testimony of Bill Jordan
Deputy Superintendent of Public Instruction
State of Washington
August 17, 1999

Introduction

I'm Bill Jordan, the Deputy Superintendent of Public Instruction for Washington State. The K–12 education system for Washington's 1 million K–12 students includes 296 school districts and 2,071 schools. I'm happy to have this opportunity to discuss Y2K concerns with you because this is an important opportunity for federal, state, and local governments to work together in ensuring Y2K compliance and assisting community efforts to be prepared for any related problems that may arise.

Where We Are

Most of the Y2K work at the state level in educational organizations has taken the form of checking internal electronic data systems and mechanical support systems to guard against potential "blow outs" and loss of important electronic data, basic heat and light systems, and vendor services. As an agency, the Office of Superintendent of Public Instruction has contacted the nine educational service districts (ESDs) to verify the activities of local districts and schools.

The ESDs have provided workshops, information, and in some instances, considerable technical assistance to help districts and schools prepare for avoiding potential Y2K problems. Generally, mid-size and larger districts have worked on checking electronic equipment and developing Y2K plans. ESD 112 at Vancouver has been very active in helping the 30 districts in their region qualify for risk management insurance. They have developed a Y2K planning manual and helped districts make plans for a variety of contingencies and scenarios that could result form Y2K problems.

Other ESDs and districts have worked in similar ways. Potential problem areas are likely to be smaller districts with limited numbers of staff and resources to deal with in-depth planning and preparation. These districts and communities need expertise and resources.

Potential Need

The focus of Y2K planning in many areas has been on checking and updating electronic data systems. Community planning has often taken the form of planning for a three-day storm. We now realize that there is the potential for a longer period of disruption and the need for a larger, coordinated effort to move toward full community preparedness.

Controlled tests of community systems reveal two things. First, there is a broad interdependence of community electronic systems. A water system may be compliant and functioning, but its interactions with other systems place a strain on both systems that can lead to failure and resulting problems. Tests need to involve the range of community systems—electronic systems, utilities, transportation, distribution systems, and all types of electrical tools or appliances. Critical needs such as heating, water, food distribution, transportation, communications, health care, and other services could be affected.

Second, many have focused on the prevention of problems but less on contingency plans and broader community preparedness. All of us fervently hope that the efforts taken to date will be sufficient to avert any disruption and crisis. Given the pervasiveness of automated electronic systems and the widespread use of embedded chips, it is difficult to guarantee that all systems will function, and it is imperative that communities are prepared to meet any problems that may arise.

Preparation for Y2K should be no different than other forms of emergency preparedness. Community preparedness for any disruption or emergency is a good thing to do, and 1999 is a good year in which to do it. Schools frequently play an important role in providing shelter, food, and supporting other needed community services. When we work together we can weather nearly any form of emergency or crisis.

Recommendations

I am recommending that federal, state, and local governments and community agencies join together actively and visibly in a careful evaluation and promotion of community preparedness. This preparedness must extend beyond the checking of electronic systems and include preparedness for related Y2K disruptions as well as other possible disaster or emergencies and would call on a community's school as a resource.

Some communities have involved groups and moved ahead. Others have not developed plans or understood the need for planning. What is needed in the next four and one-half months is the following.

- Citizen education programs that can provide guidance to citizens about the potential problems that might be experienced.

- Local contingency planning and preparedness efforts that can give citizens a sense of confidence that they will not be left alone to cope with problems or emergencies.

- Controlled community preparedness tests that build coordinated community interagency capacity to deal with emergencies.

- A coordination of federal, state, and local actions that can provide early responses to possible needs for water, food supplies, fuels, and emergency services.

- Provision of guidance to families as to ways of preparing for and responding to problems.

It is possible that few problems will occur, but it is also possible that some may face disruptions and hardships. Preparedness will not be wasted effort because potential hardships may be avoided or reduced, and communities will be better prepared for other potential emergencies. One of the tasks of all levels of government is to care for citizens. Building coordinated federal, state, and local awareness and capacity for community preparedness is one way this role is fulfilled.

Mr. HORN. Well, we appreciate that. We haven't really had much testimony from the K–12 sector, so I'm delighted to have your statement.

Mr. Bergeon, consultant with NueVue International Audit 2000.

Mr. BERGEON. Chairman Horn, Representative Dunn, it's a great pleasure for me to be here today.

I think I have the unenviable task of addressing the small to medium business environment, which I've been consulting with for quite some time. I'd like to say that given my experience here in Seattle, there's probably no city in the country I'd rather be in when the clock turns over.

In the last few years, my work has been going on with various commercial banks, and I've been very pleased with the kinds of things I've seen coming through the Federal Reserve and all of the other agencies as part of that movement.

I think that we are about to see probably the proof of the pudding here in the next few months when the banks are going to be asked to really evaluate their credit customers and to actually do something about it. It's already been a very active movement by the banks, and that has made a world of difference in the small and medium business area being aware and making the move, but there's still a long ways to go in the small business area.

Just a few months ago I had an opportunity to talk with a number of ports. And I've worked with the Port of Tacoma and Port of Seattle and know they're moving along extremely well, and they should be ready well before the year 2000 arrives.

But in talking with many of the ports around the area, I found that most of them have started relatively recently, and they have a certain amount of work that they have to get done and to finish that up before the end of the year. So we still have, in our port areas, both with the smaller airports and the marine facilities in and around the northwest, still have a lot of work to do.

I have had an opportunity to work with a number of different business areas. I will give you an example of a trucking firm that is in the Seattle area. I found that they were aggressive. They had moved on their problem. They had two things to worry about: APC and their accounting software. They replaced both of those.

But in going over with them what their exposures were to the Y2K, we found something like 19 systems over which they were dependent but had absolutely no control. What was even more disconcerting is they had no idea about how to approach them and had no idea of how to perform or build a contingency plan. So we still have that kind of an issue that we have to deal with in the small business arena.

I also reviewed a small manufacturing company that was Y2K compliant, and in doing the review, found that they had missed seven embedded systems, which reinforces the fact that most of these companies that are doing the work by themselves because they can't afford outside consultants are potentially going to miss some things that maybe a "professional"—and I want to put that in quotes—would capture.

I've also worked with the fishing boat industry and had an opportunity to tour a number of fishing boats and look at the computers and equipment on board the fishing boats. I'd like to tell you that the navigation systems are, for the most part, redundant for the larger ships, and even for some of the smaller ones. So that's not going to be an issue unless they all give different readings.

But for the most part, the fishing boats are heavily dependent upon equipment with embedded systems, and there has not been a lot of communication from vendors to the fishing boat operators within the last year.

I've also had an opportunity to talk with one of those fishing boat operators and have reviewed their home system, their at-base system, and found that while their programmer had gone through and said that they were compliant, he was, in fact, unaware of the scope of testing that needed to be done in order to achieve compliance.

So again, there is a difference when you get into the small business area about the depth of knowledge and the amount of work that has to be done.

I think that I would like to reinforce the concerns about the December timeframe and potential reaction by the public, both in the food area and in the petroleum area. There are strong concerns amongst the business people about potentially not having enough supply to meet demand, that they could get out of hand. Education is important and essential, and we do have to get out there and do more for them on that particular problem.

I am also concerned, as my co-speaker from Microsoft said, about the amount of business that's moving from the first quarter of 2000 into the last quarter of 1999. For many small businesses, this could have an impact, because their cash-flow issues are stronger than most of the larger companies'.

With that, I'd like to conclude my comments.

[The prepared statement of Mr. Bergeon follows:]

Testimony before the Subcommittee on Government Management, Information, and Technology – 17 August 1999

By Richard Bergeon

Managing Consultant for NueVue International LLC; Vice President of Audit 2000, Inc., and an Associate of the Discovery Institute

---

Let me start by saying that it is an honor to appear before members of the committee as well as my local representatives.

In the seven years that I have been involved with Y2K problem solutions, domestically and internationally, my anxiety levels have ranged from non-existent to a "cold sweat", tapering off to nervousness. I never became an alarmist. To this day I don't feel it is appropriate to "run for the hills!" However, since April my anxiety levels have started to increase exponentially.

In the first quarter of this year I was actually at ease. The Federal government had finally weighed in and pressure was being applied across the board. Community action groups were springing up all over as concerned citizens started to make contingency plans. Local utilities were presenting their state of readiness and working with major agencies in joint contingency planning. The media seemed to have stopped exploiting the Y2K issue and had started to inform the public about real and imagined risks.

In the second quarter I saw numerous groups representing industries, that had previously had not a clue about the Y2K risks to themselves, suddenly reporting tremendous strides and even significant levels of Y2K compliance. I saw reports of huge budgets that had been still not been spent. I heard firms and government agencies, which had been on record as falling further behind (which is normal), suddenly reporting compliance on schedule.

I have been the information technology industry for over thirty years. During most of this time I was responsible for managing projects or managing those who led project teams for large private companies. I was not always successful as a project manager and became all too familiar with the 95% rule. (Projects rapidly reach the point of 95% completion and then hang there for what seems forever.) I am a witness to organization defensive processes that do not permit upper management to hear bad news. I have seen reports of problems rewritten and learned how to make reverses seem like progress.

As an information technology person I see in the sudden progress a familiar pattern. I see a rush by managers to meet a deadline instead of getting the job done right. I see managers declaring victory and moving on leaving the problems that will show up later for someone else worry about. As deadlines approach, and resources get tougher to obtain, the tendency is to curtail testing. The tests focus on "what should happen" and ignore the "what if" scenarios and the "what shouldn't happen". In many instances testing is just skipped all together. Programs are returned to production and a "watch" is placed on them.

In one recent survey reported in the news, 38% of the information systems managers responding reported experiencing errors in their systems or those of their vendors. And this is while processing 1999 data. I have seen other news reports about systems that were brought in to replace Y2K non-compliant systems being so filled with bugs that they had to be removed and the old system restored. There have been numerous reports of situations that, when supposedly compliant systems were closely examined, many still had not yet been tested, and others (that were carefully audited) turned out to contain numerous errors that had not been caught. Some "compliant systems" were still being tested behind the scenes.

I am becoming concerned that more and frequent failures will occur in the coming months that will weaken public confidence and lead to panic. I would like to share some of my experiences.

- In January I was asked if I wanted to respond to a request for quote on a government agency contract to perform an independent validation and verification (IV&V). I declined because the agency limited the contract to 80 hours of work to review 40 application systems that were developed and still managed by four contractors (in some instances remotely). These applications were part of a highly integrated environment. Depending on the number of interfaces the contract should not have been for less than 160 hours (four hours per application), eight hours for each operational site, and two hours to review each application interface.

- In March I completed an IV&V of an international bank that performed commercial lending in the US. The bank was in great shape meeting or exceeding every one of the Federal Reserve's guidelines. But a few things bothered me about general banking credit risks:

  1. Many loans are syndicated. One bank leads and the others share in the loan. Only the primary has direct contact with the borrower and the others depended on the primary to gather the information. There is little, other than constant pestering, that the secondary banks can do assure themselves that the loan is safe.
  2. While some loans are on a "watch" list there is little motivation to accelerate a loan if the borrower falls behind in its Y2K preparations. A bank that takes action it could receive a black eye in the business community. Another bank might easily pickup the loan (albeit with a higher interest rate) and no one would be the wiser until the fate of the borrower is revealed next year. If the borrower survives, the first bank might be sued for the costs and damages incurred in getting the second loan. Many of these loans are to the small and mid-size firms which have a poor track record on Y2K compliance.
  3. All banks are asking their loan officers (the ones who interface with clients) to be responsible for overseeing the borrower's Y2K compliance efforts. While they have undergone training it is hard to imagine someone who does not stay abreast Y2K risks can do an adequate job of progress assessment. They rely on the knowledge and ability of the borrower to assess its own progress.

  What would or could the bank do to enforce Y2K compliance if the time came? If all the banks acted in unison to mitigate losses in the fourth quarter the economic impact could be dramatic. Shades of "Catch 22!"

- Only two months ago I had a conversation with a representative of a another bank about their Y2K contingency planning activities. The individual proudly reported completion. When I delved further I was surprised to find that their plan only covered on-site computer problems and did not address long-term power outages, civil unrest, foreclosures on risky loans, loss of communication with their home office, etc. etc.

- Recently I spoke at an Association of American Port Authorities conference about Y2K contingency planning. Most of those in attendance said they had not started contingency planning and many had not yet completed work to become Y2K compliant. Many were unaware of the topics that needed to be addressed in contingency planning. Most had not even considered creating one.

- Several months ago FEMA told people to prepare for Y2K as if it were going to be a three-day storm. A reasonable analogy in the sense of power outages and apparently responsible and certainly one that diminished any sense of panic. Many community action groups disbanded. Why? Nearly all of those who join those groups are reasonably able to deal with a three-day storm. Many, including myself, have weathered three-day power outages without financial impact and only minor discomfort. Was the message a responsible one? Only time will tell. Can FEMA regain the momentum? It has most likely lost its credibility.

I also have some lingering concerns that contribute to my sudden increase in anxiety.

1. Most of the people I talk to report they "intend" to stock up on food and water for Y2K. A recent survey said 30% of the people will stock up on food. If even 10% of the population rushes the grocery stores in December we could see a sudden surge by at least another 30% and then panic buying as shelves empty.

2. Most people I know intend to fill their auto gas tanks in the last week of December and some are buying storage cans. In the Northwest we already have a weakened supply chain caused by refinery and pipeline shutdowns. If gas lines appear in the western states panic buying is just around the other side of the pump. The media could spread the panic across the US. Depleting the supply chain will only exacerbate the problem. Failures in pipelines, refineries, international shipping, power supplies, and/or telecommunications could severely retard restoration of normalcy.

3. We have become a just-in-time society. More and more of our work has become reliant on communication and transportation. Failures, even short-term failures, could cause catastrophic events. Nursing homes do not normally maintain enough medication, linen or power backup to sustain their charges for more than 24 hours. Can they outlast power-outages, gasoline shortages, telecommunications brown-outs? With community help they can. But, how long will it take the community to mobilize itself now?

4. The power industry is practicing grid shutdowns and the reports are that everything is "cool". The feeling is left that the power industry is on top of things. What they don't tell us is that they just don't know what is going to happen. They don't know if the grid will collapse in one or many places at once because they can't test it. Further they cannot test restoring power on the grid until its shutdown and Y2K is upon us. How long will shutdowns last? The power companies are confident of three days at best. In a snowstorm? (I don't need to remind everyone about the current weather turmoil.) What about when communications are in turmoil, or when they unable to fuel their vehicles? What about nuclear reactors where the systems are on failsafe and can be counted upon to shutdown reliably for any problem? If they shutdown how long will it take to restore operation?

5. The telecommunications industry is expecting the worst of all "mother's day" scenarios. Internet watching around the world is expected to tie up many circuits, to either

> experience the millennium or watch for a Y2K catastrophe. An abnormal number of millennium well wishers and millennium doom worriers will attempt to use the phones. Together they are expected to create a massive demand that cannot be met. Millions of people trying to make connections or reconnect can lead to the belief that the system has failed.

We are here today to talk about what government can do. The government has two responsibilities to the populace. The first is to protect it. The second is to promote its welfare. Both have positive and negative aspects and sometimes they are in conflict. To promote public welfare (read that economic condition, individual rights, financial security) it is sometimes best not to reveal threats especially ones that can be dealt with quietly. Responsible government does not panic the public. Too many people lose and there are repercussions throughout the community.

Knowledgeable people act responsibly. Prepared people know what to do when the worst happens. The rest panic. I suggest government start preparing the public, informing them reliably and with concern, that the problem is real and that difficulty will be encountered. They should learn to expect slowdowns and system failures domestically and internationally. This warning message can be delivered with a reassurance that any problems will be short-lived and that economically the U.S. will remain sound.

Thank you for your attention.

Mr. HORN. Well, thank you, Mr. Bergeon. Are you familiar with the pamphlet that the Small Business Administration put out on this?

Mr. BERGEON. Yes, I am. I'm very glad to have seen it. I wish it had come out about a year ago.

Mr. HORN. Well, it came out last July, actually, is when they first showed it to me.

Mr. BERGEON. I'm thinking the year earlier.

Mr. HORN. Did you find it useful?

Mr. BERGEON. Yes. I think most of the companies that have seen it were awakened to things that they hadn't realized. And as I said, I just wish it had come out probably a year ahead of when it did.

Mr. HORN. Did it tell them enough to deal with the remediation, or was something else needed?

Mr. BERGEON. There again, most of them are trying to do the work on their own, with the resources that they have available or can bring to bear. Not all of these resources are knowledgeable or skilled. The SBA pamphlet has done a great deal to remediate that problem, but there are still issues that come up that they don't know how to address.

Mr. HORN. Let me ask the question I've asked the two previous panels. If you could rethink where you've been on this, what from the management side would you now change and go at it in another way if you had to do it over?

Mr. BERGEON. Well, I started in the Y2K business in 1992, and I started with big businesses, because consulting companies, for the most part, get the attention of big businesses and make most of their money with big businesses.

I would like to have started with the small business arena probably about 4 years ago, and I would think that if we had this to do over again, I would do that.

Mr. HORN. Mr. Jordan, what would you do if you had to roll back the clock and say, "Gee, we should have done this at this point in time"?

Mr. JORDAN. We should have spent more time on better communication and contingency planning.

Mr. HORN. Now, when you say "contingency planning," what are you thinking of?

Mr. JORDAN. Well, school districts and schools are very dependent on vendors, outside sources, to keep us working. And we should have started earlier on making plans for the checking of integrated systems and vendor sources and contingencies if our food supply doesn't come in for food service or fuel supply doesn't come in to transport our buses.

Mr. HORN. With your overview of education in the State, did the major cities, such as Seattle, Tacoma, others, have a plan in the city school systems? And how would you relate what was happening in the rural school systems? And I'm just curious, from your perspective, what do you see there and what should they have done earlier?

Mr. JORDAN. Probably the best answer—I can defer to one of our previous speakers regarding perhaps what's happened with the city of Seattle or King County in their relationship with the school district.

My feelings regarding rural school districts are that they are in need of resources to find people to check out systems or relying on the educational service district to provide expertise or support. So they are probably in a position of less preparedness than the larger districts.

Mr. HORN. Well, I'm thinking of when they were wiring classrooms. A lot of this was volunteer effort by people that were familiar with computers and wanted to help out and provide those opportunities.

And I guess Mr. Jones—we might ask him. Microsoft is, without question, probably the largest computer firm in America in terms of software?

Mr. JONES. Second largest.

Mr. HORN. Second largest. Who is the No. 1?

Mr. JONES. IBM.

Mr. HORN. Big Blue is still No. 1.

Anyhow, I just was curious. You probably remember that volunteer effort to wire different rooms in schools. Was there anything like that applied to the remediation situation on the year 2000?

Mr. JONES. Well, there have been several things done in that area. I mean, we've worked with a number of school districts to wire them, the first thing.

Second, there have been nonprofit organizations in Seattle, such as Empower, and what they've done is they've worked with all the other nonprofits to prepare them for the year 2000.

Y2K for nonprofits is a huge challenge. They don't have the technical expertise nor the financial means to do a great job of preparedness, so they're relying on industry or other nonprofits that specialize in supporting them in those areas.

Mr. HORN. Ms. Enticknap, what's your feeling on it? If you could roll back the clock and say, "Gee, we should have done it this way," what would you have done differently?

Ms. ENTICKNAP. Financial institutions benefited from a very active regulatory support, and so the Federal Financial Institutions Examination Council [FFIEC], came out very early with recommendations. We had already started work. So we, as I say, benefit from a very active regulatory environment, shall we say, so we've been ready.

Mr. HORN. Well, you're in the corporate culture now of two major banks. Was there a difference between how Seattle versus Bank of America had approached this from?

Ms. ENTICKNAP. No. Actually, we've been part of Bank of America since 1983, and we just didn't change our name. So we've been part of Bank of America and have played an active role in the overall corporate planning process and remediation process.

Mr. HORN. Mr. Aikens, how about Boeing? Does Boeing ever make a mistake? Would you ever go back?

Mr. AIKENS. I think we've made a mistake.

Since we started early, the one thing that I think would have helped is if we could have resolved the fear that the suppliers had. Somehow we needed to resolve that, because it limited the communication. Although we started in 1993, working with our suppliers in 1994, they were still very reluctant to share. And if we could have worked to eliminate that fear, I think that would have been better.

Mr. HORN. Well, that's a good point.

Allow me just to go through some of these cards that the audience has provided. I guess, Mr. Jones, here's one for you: please explain the Y2K brochure Microsoft plans to mail out and who will receive it.

Mr. JONES. The brochure is essentially called "Action for Small and Medium Businesses and Consumers." Basically, the criteria for who will receive that mailing is anyone who has registered a product since 1995. For businesses, enterprise businesses, we then reduce the duplication in names and only send one mailing to the Y2K program manager of a specific enterprise.

Mr. HORN. Are there any Microsoft products that are not Y2K compliant?

Mr. JONES. Of the 3,200 we've tested, about 2 percent, or roughly 80. And for those products, we have either an upgrade path or a work-around available.

Mr. HORN. Recent reports illustrate that small to medium-sized businesses are not doing enough to prepare. What is your confidence level—I think it's really directed at you, Mr. Bergeon—as to is it a low confidence or high confidence in terms of the supply chain?

Mr. BERGEON. Again, in dealing with the small and medium businesses, we're going to cover a lot of territory. And let me break it down into two groups first.

The medium-sized businesses, I think, are coming along extremely well. I have a high degree of confidence that most of them will be in pretty good shape by the end of this year. They will be working heavily into the last quarter.

Small businesses, it's about 50 percent right now. I'm seeing more and more interest, but still a reluctance to do anything at this point, because they've got other issues they're dealing with and they still have cash-flow issues. Many of them still are not aware of things like contingency plans.

And they have expressed a great deal of fear about why should they do something when they still expect some of the other systems to fail around them. So there's still a lot of hesitancy or a lot of disbelief in government, et cetera. I've heard it said the "close enough for government work" phrase all too often. And so my confidence, I think, with the small businesses is not as high. It's only about 50 percent right now.

Mr. HORN. How about the supplier confidence you have, Mr. Jordan?

Mr. JORDAN. With the State of Washington, which probably most of our school districts rely on for information services and data services, we have a high level of confidence.

With some local vendors, they are also expressing reluctance to give us assurance that they will be able to supply us with our needed services because they are not sure that they will be supplied with the materials and the backup that they have.

So in some of our larger systems, we feel very confident; in others—and depending on the size of the business—not very confident.

Mr. HORN. Ms. Enticknap.

Ms. ENTICKNAP. We are confident that the small businesses that we are working with, we've tried to provide as much information as possible, including guides, checklists and seminars, both for our small and medium-sized businesses. So we've tried to outreach to those businesses to provide as much information as we could.

Mr. HORN. Since we've got you here, what impacts could noncompliant international banks have on your operations?

Ms. ENTICKNAP. We've been working very closely with the partners internationally that we use, including testing, and are confident that we will be able to manage any risks as they come up.

Mr. HORN. What about the confidence you have in your suppliers becoming compliant?

Mr. AIKENS. We have something like 33,000 suppliers, and we've been working to get that down. We have less than 100 that have not responded exactly like we want, and we're dealing face to face with those. We are confident that we will resolve that issue.

Mr. HORN. And we have a number here for Mr. Jones. Do you want to comment on the suppliers?

Mr. JONES. I do, actually. An inverse view of that is Microsoft is a supplier to many of the people who have testified here today. And to quantify that for you, we have received approximately 9,000 requests for information from Microsoft per week. And we expect by the time the year ends, we will have processed well over 1.4 million requests for information. And that's above and beyond the website utilization that we have.

Mr. HORN. Someone wanted us to be more specific, and the request is this: are Windows 95 and Windows 98 compliant?

Mr. JONES. Windows 95 and Windows 98 are both compliant. There is a software update available.

Mr. HORN. Is Office 97 compliant?

Mr. JONES. Office 97 is compliant with software updates.

Mr. HORN. And here is a nonprofit volunteer in the community: please explain the Empower program to help nonprofits meet Y2K compliance.

Mr. JONES. Certainly. Empower is a local nonprofit organization designed to support other nonprofits through technology. They have database analysts, programmers and developers on staff. They launched a program called the Y2K Data Service here in Seattle, and that ran about 6 weeks ago, and they went and touched about 200 nonprofit organizations, and they verified the readiness of their PCs and installed the software updates or any patches that were necessary.

They had volunteers from Microsoft, from Boeing, from many of the large organizations within the Seattle area. They're going to do another one of those later in the year. And "www.Empower.org" is their website.

Mr. HORN. The final two questions are for Mr. Aikens, and they're along the line of the ones for the banks, and that to you is: what contingency plans are being made for employees in high-risk areas, like Russia, in terms of Boeing personnel, Boeing customers, whatever, in terms of the year 2000 and working with Russia?

Mr. AIKENS. Well, we have a normal contingency plan for all of our people, and Y2K is no different. We have emergency operation centers in 12 States, and also abroad. So we work with each one of those countries, and our people will be protected.

Mr. HORN. I just happened to visit your Sea Launch facility in my hometown of Long Beach this last week, and it was really impressive, with Russian, Ukrainian, Norwegian, United States, and United Kingdom cooperation. That's really a great endeavour.

Mr. AIKENS. It is a very interesting site.

Mr. HORN. We'd be glad to have you send some 737 production down there, too, before I leave town, please.

"What can you tell us about the Global Positioning System readiness on August 21st and 22nd, 1999?" says one member of our audience.

Mr. AIKENS. We're completely ready. And what we have done is we've contacted the vendors that have the information, at least have the satellites, and we have demanded—it sounds pretty strong—that all of those systems be ready. Boeing has run through its tests, and we are completely satisfied that there will be no problem with the Global Positioning System.

Mr. HORN. I thank you. And I now yield to Representative Dunn for the questions she has, and we're delighted she is with us here.

Ms. DUNN. Thanks very much, Mr. Chairman.

Mr. Jones, you mentioned a couple of times, or it was mentioned on your behalf, that you've worked a lot with nonprofits. And we haven't heard anybody testify from the nonprofit sector. And I am most curious myself, having been very involved with this sector in most of my background, what kind of progress are the nonprofits making toward compliance for Y2K?

Mr. JONES. I would rank them at the bottom of the list, with enterprises being most compliant and nonprofits being the least. That's singularly the area that concerns us the most. They typically have outdated technology, which, of course, induces more areas for Y2K liability. And while they are turning their attention to Y2K now, it is relatively late for those organizations.

Ms. DUNN. So we should pay some attention there.

Mr. JONES. Absolutely.

Ms. DUNN. I think that's important, Mr. Chairman.

Let me ask you, in general, a question I know Mr. McDermott had asked earlier as I was outside for another meeting on the impact on somebody's home. And I think he phrased it in terms of whether his answering machine would work or not.

What else do you see is going to be a problem for the ordinary person going through his life on the 1st day of the new millennium? What will they notice?

And then I have another followup question I want to ask a couple of you on that. Anything that occurs to any of you in any order.

Mr. JONES. From the PC standpoint, I'll address that component. Depending on how you use your PC—say you use your PC primarily to surf the web or play games—by and large, you could do nothing, turn your PC on on January 1st, and you'd be just fine.

If you use your PC for complex calculations or checkbook management, budget management, then certainly you need to take some preparedness steps. On average, we're seeing those steps take about an hour to do in the home.

Ms. DUNN. Is there someplace where people can get information on how to do that?

Mr. JONES. Microsoft has a great website, of course.

Ms. DUNN. Anything else? Anything you're worried about, your wife is worried about, your husband is worried about, your children are worried about?

Mr. BERGEON. Having moved into a condo in downtown Seattle, I had a lot of things to worry about, including elevators and environmental control systems, so we did do some checking.

We've found that if you have an environmental control system that was purchased within the last few years, you're pretty safe. But most of the houses have had environmental control systems that were installed some time ago, and some, some small percentage, do have some computer embedded chips in them. It's not clear whether or not those are going to be prepared or not. And I haven't done a study of them, but that is a concern that some homes might have.

Ms. DUNN. Anybody else?

Mr. AIKENS. Well, we have a very extensive program within Boeing for all of our employees that have PCs. And we have a PC assistant that will allow them to take a look to see if their computer is Y2K-ready. They can take this kind of information to the home as well.

And in addition to that, the Boeing Employees Credit Union, which is not a part of Boeing, has sent out a list of things that they need to do. And in that way, they will check with Microsoft or any of the other vendors as to what needs to be done. By and large, we think that it really won't be that much of an impact on the homes.

Ms. DUNN. Good. Thank you. I have just one last question. There was something that alarmed me that I heard earlier in this hearing, and that was when one of the folks who was testifying said he'd heard there were going to be a couple of movies coming out on the Y2K.

And you can translate that very quickly, having been through that era of every possible disaster in the world becoming part of a movie. And it's our responsibility here, all of us who have taken part in this hearing today, to make sure that the institutions we're affiliated with are compliant.

What happens, though—because we know the psychology of this is going to be very important, especially in the possibility that you run into all the time, Mrs. Enticknap, of people taking their money out of banks, or you run into, Mr. Aikens, of people not flying on airplanes—what happens and what is the response? And are you prepared with a contingency plan if something like this happens toward the end of the year? We've got a November release for some big movie. How are we going to calm people down and help them understand, especially seniors, who worry a lot about things like this?

Mr. AIKENS. I'll take it. Naturally, Boeing is a primary target to have a 747 crashing into the Empire State Building. These kinds of things come up all the time. And what we think is the best way to combat that is with education, and that's where we think that our outreach program is very effective.

The contingency plan is that there is not much we can do about Hollywood doing things like this, but we think education is the answer. And that's what we want to be sure that we tell the public—here's what we're doing—and let's leave it at that.

Ms. ENTICKNAP. From the bank's standpoint, we have an active communication program under way. We will be sending out and continue to send out statement stuffers. Again, people tend to not read their statements, so we also have information on our websites and also in our banking centers. And we also are working with the Federal Reserve. The Federal Reserve is printing an additional $50 billion of currency for the end of the year, and all banks are working together to make sure that we're monitoring cash usage.

But more importantly, we're working with senior citizens and others to really understand the implications of taking their money out, and urging people to recognize that the safest place for their money is a bank.

Ms. DUNN. Anybody else have any comments?

Mr. JORDAN. We agree that education is critical to making sense of this. And one of the things we'd like to stress is that this is an opportunity for community agencies—profit, nonprofit, big and small business—to come together and clearly state for the community what is and what isn't. That will belay a lot of fear and cut through any media marketing that might go along with the production that you scenario.

But we believe that if a community gets together, and each agency says we've done this, this, this, and this, and get that out to their local people that trust them and rely on them every day, that would have a big impact.

Ms. DUNN. Thank you.

Mr. HORN. Thank you very much for coming, Ms. Dunn. She does a great job for you in Washington.

Let me thank a lot of people that have been involved in this hearing. We'll start with the two Members of Congress and their staff. Congressman McDermott and his Seattle district office staff has been helpful—Damian Cordova, legislative assistant, Jane Sanders, the scheduler.

And Congresswoman Dunn's Washington and Mercer Island district office staff, Susan McColley, district director, Kara Kennedy, the press, Doug Badger, legislative director.

And for the Discovery Institute, which is also our host in Seattle, obviously president Bruce Chapman, who has been a great public servant, both nationally and in this State and in this city, I've known him for 40 years as a person of honor and integrity; Nancy Sclater, the vice president; Rob Crowther, the public and media relations; Steve Jost, events coordinator.

And our faithful court reporter, Jeff Wilson. And then the staff of the Subcommittee on Government Management, Information, and Technology which has done a great job for the last 6 years. J. Russell George, staff director and chief counsel, is seated practically outside of the room there in back; Matthew Ryan is to my left and your right, he's the senior policy director that worked on the hearing.

And then we have a very fine young lady who is an American Political Science Association congressional fellow with Congress for a year, and her full-time employment is career servant for the National Security Agency, and that's Patricia Jones.

Patricia, are you here? Well, she had to leave.

Chip Ahlswede, I believe, is here, staff assistant; and Grant Newman, the committee clerk. Grant, there they are. They're all in the back row.

So I want to thank you all. I want to thank the people of Seattle and your experts that we had as a sounding board, shall we say, for our various aspects of the Y2K problem. You've put a lot of good information in the record today, and we will make use of it and share it with other communities. Thanks for coming.

With that, we are adjourned.

[Whereupon, at 12:20 p.m., the subcommittee was adjourned.]

○